

LOAN COPY

LIBRARY
DOCUMENTATION CONTROL CENTER

ORDER

1600.28

NATIONAL SECURITY INFORMATION
TITLE OF DIRECTIVE May be typewritten or set in type



LIBRARY USE ONLY

February 5, 1980

DATE: May be typewritten or set in type

DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

ADVANCE COPY

1-101(CB)-312-Y(2E)-312-2(2E)-3

Revised By: 102-20012

199. RESERVED

93 (and 94)

CHAPTER 9. VISIT CONTROL	95
SECTION 1. GENERAL PROVISIONS	95
200. Definition of Visitor	95
201. Incoming Visits	95
202. Visitor Categories	95
203. Identification	98
204. Visitor Logs	98
205. Restrictions of Movement	98
206. Recordings and Photographs	98
207. Report of Unusual Visitor Interest	98
208. Outgoing Visits	99
209. RESERVED	99
SECTION 2. INTRA-FAA VISITS	99
210. Discussion	99
211. Intra-FAA Visits	100
212. RESERVED	100
CHAPTER 10. COMPROMISES AND SECURITY VIOLATIONS	101
213. Summary of Controls	101
214. Violations of Security Directives	101
215. Initial Reporting and Responsibilities	101
216. Administrative Inquiries	102
217. Additional Notification and Investigation	102
218. Actions Subsequent to Investigation	102
219. Classification of Reports	103
220. Cryptographic Information	103
APPENDIX 1. EQUIVALENT FOREIGN AND INTERNATIONAL PACT ORGANIZATION SECURITY CLASSIFICATIONS (6 Pages)	1
APPENDIX 2. FORMS LIST FOR ORDER 1600.2B (1 Page)	1

SECTION 3.	SPECIAL PROCEDURES FOR HAND-CARRYING CLASSIFIED INFORMATION ON COMMERCIAL PASSENGER AIRCRAFT	85
178.	Prohibitions	85
179.	Basic Requirements	86
180.	Procedures for Carrying Classified Information in Envelopes	86
181.	Procedures for Transporting Classified Information in Packages	86
182.	Documentation	86
183.	RESERVED	87

SECTION 4.	DISPOSAL AND DESTRUCTION OF CLASSIFIED MATERIAL	87
184.	Discussion	87
185.	Authorized Disposal	87
186.	Procedures Leading to Destruction	88
187.	Methods of Destruction	89
188.	Destruction Officials	89
189.	Records	89
190.	RESERVED	90

CHAPTER 8.	FOREIGN GOVERNMENT AND INTERNATIONAL INFORMATION	91
------------	---	----

SECTION 1.	CLASSIFICATION, DECLASSIFICATION AND MARKING OF FOREIGN GOVERNMENT INFORMATION	91
191.	Definition	91
192.	Classifying Foreign Government Information	91
193.	Duration of Classification	92
194.	Declassification of Foreign Government Information	92
195.	Marking Foreign Government Information	92
196.	RESERVED	92

SECTION 2.	INTERNATIONAL INFORMATION	92
197.	NATO and CLATO Classified Information	92
198.	Control of International Organization Information	93

	<u>Page No.</u>
154. Other Factors	69
155. Supervision of Storage Containers	70
156. Identity of Storage Facilities	70
157. Control of Combinations	70
158. Special Precautions	72
159. Lock-Out	72
160. RESERVED	72
 SECTION 2. CUSTODY AND AREA CONTROLS	 73
161. Basic Provisions	73
162. Care During Emergencies	74
163. Area Controls	75
164. RESERVED	76
 CHAPTER 7. REPRODUCTION, TRANSMISSION AND DESTRUCTION OF CLASSIFIED MATERIAL	 77
 SECTION 1. REPRODUCTION	 77
165. Discussion	77
166. Authorization	77
167. Accountability for Reproduced Copies	77
168. Markings	78
169. Controls over Reproduction Equipment and Areas	78
170. RESERVED	79
 SECTION 2. TRANSMISSION OF CLASSIFIED MATERIAL	 79
171. Preparation and Packing Requirements (Mailable Material)	79
172. Preparation and Packaging Requirements (Non-Mailable Bulk Items)	81
173. Methods of Transmission	81
174. Advance Notice and Bills of Lading	83
175. Use of Telecommunications	84
176. Additional Requirements in Connection with Visiting	84
177. RESERVED	85

CHAPTER 5. ACCESS, DISSEMINATION, AND CONTROL OF CLASSIFIED INFORMATION 51

SECTION 1. ACCESS 51

- 130. Principal 51
- 131. Determination of Trustworthiness 51
- 132. Continuous Evaluation of Eligibility 51
- 133. Determination of Need-to-Know 52
- 134. Revocation or Rescission of Security Clearance 52
- 135. Access and Dissemination Requirements in General 52
- 136. Special Access Programs 53
- 137-138. RESERVED 53

SECTION 2. DISSEMINATION 53

- 139. Dissemination within the Executive Branch 53
- 140. Dissemination outside the Executive Branch 53
- 141. Dissemination through Meetings 62
- 142. RESERVED 63

SECTION 3. CONTROL OF CLASSIFIED INFORMATION 63

- 143. General 63
- 144. Security Control Point 63
- 145. Records 64
- 146. Working Papers 65
- 147. Additional Top Secret Controls 66
- 148. Material Which Is Hand-Carried to or from an Activity 66
- 149. Document Control Station 66
- 150. Exceptions for Unique Material 67
- 151. RESERVED 67 (and 68)

CHAPTER 6. STORAGE AND SAFEKEEPING OF CLASSIFIED MATERIAL 69

SECTION 1. STORAGE AND STORAGE EQUIPMENT 69

- 152. Use of Storage Containers 69
- 153. Types of Containers Authorized 69

	<u>Page No.</u>
Data Processing Tapes	44
104. Pages of ADP Listings	44
105. Decks of Accounting Machine Cards	44
106-109. RESERVED	44
 SECTION 4. CLASSIFICATION AUTHORITY, DURATION AND CHANGE MARKINGS	 45
110. Declassification and Regrading Marking Procedures	45
111. Applying Derivative Declassification Dates	45
112. Upgrading	46
113. RESERVED	46
 SECTION 5. ADDITIONAL WARNING NOTICES	 46
114. General Provisions	46
115. Restricted Data	46
116. Formerly Restricted Data	47
117. Intelligence Sources and Methods Information	47
118. Dissemination and Reproduction Notice	47
119. Other Notations	47
120. RESERVED	47
 SECTION 6. REMARKING MATERIAL CLASSIFIED UNDER PREVIOUS EXECUTIVE ORDERS AND DIRECTIVES	 47
121. General	47
122. Foreign Government Information	48
123. Remarking Documents or Material Marked "Subject to the General Declassification Schedule" or "Advanced Declassification Schedule"	48
124. Remarking Documents or Material Marked As "Exempt from the GDS" or Not Marked with Any Declassification Instructions	48
125. Remarking Documents or Material Marked "Group 4"	48
126. Remarking Documents or Material Marked "Group 1, 2 or 3" or Not Group Marked	49
127. Earlier Declassification	49
128-129. RESERVED	49 (and 50)

	<u>Page No.</u>
CHAPTER 4. MARKING OF CLASSIFIED INFORMATION	33
SECTION 1. GENERAL	33
80. Designation of Classified Information	33
81. Marking of Documents in General	33
82. Original Classification	33
83. Derivative Classification	33
84. Special Notations	34
85. Identification of Classification Authority	34
86. RESERVED	32
SECTION 2. SPECIFIED MARKING REQUIREMENTS	34
87. Overall and Page Marking	34
88. Major Component Marking	35
89. Portion Marking	35
90. Subjects and Titles	35
91. Unclassified Material	36
92. RESERVED	36
FIGURE 1. COMMONLY USED MARKINGS	37-38
FIGURE 2. SAMPLE CLASSIFIED LETTER	39
FIGURE 3. SAMPLE LETTER OF TRANSMITTAL FOR A CLASSIFIED DOCUMENT	40
FIGURE 4. SAMPLE CLASSIFIED MESSAGE	41
SECTION 3. MARKING MATERIAL OTHER THAN DOCUMENTS	42
93. General Provisions	42
94. Transmittal Documents	42
95. Electrically Transmitted Messages	42
96. Files	43
97. Translations	43
98. Charts, Maps and Drawings	43
99. Photographs	43
100. Transparencies and Slides	43
101. Motion Picture Films	44
102. Recordings	44
103. Electrical Machine and Automatic	44

Page No.

SECTION 4. INDUSTRIAL OPERATIONS	24
58. Classification in Industrial Operations	24
59. Independent Research and Development	25
60. Other Private Information	25
61. RESERVED	25 (and 26)
CHAPTER 3. REGRADING CLASSIFIED INFORMATION	27
SECTION 1. GENERAL PROVISIONS	27
62. Principal	27
63. Systematic Review for Declassification	27
64. Mandatory Review for Declassification	27
65. Submitting and Handling Requests for Mandatory Review	28
66. Classification Reviews under the Freedom of Information Act	28
67. Initial Classification Reviews	29
68. Remarking of Material	30
69-71. RESERVED	30
SECTION 2. DECLASSIFICATION OF TRANSFERRED DOCUMENTS OR MATERIAL	30
72. Material Officially Transferred	30
73. Material Not Officially Transferred	30
74. Transfer for Storage or Retirement	31
75. RESERVED	31
SECTION 3. REGRADING	31
76. Raising to a Higher Level of Classification	31
77. Classification of Information Previously Determined to be Unclassified	31
78. Downgrading	31
79. RESERVED	31 (and 32)

CHAPTER 1	CLASSIFICATION OF NATIONAL SECURITY INFORMATION	15
SECTION 1.	RULES GOVERNING CLASSIFICATION OF INFORMATION	15
30.	Principal	15
31.	Classification Categories	15
32.	Classifying Information Only	15
33.	Material Produced in FAA Containing Classified Information	16
34.	Accountability of Classifiers	16
35.	Classification Approval	16
36.	Classification Planning	16
37.	RESERVED	17
SECTION 2.	CLASSIFICATION PRINCIPLES, CRITERIA, AND CONSIDERATIONS	17
38.	Reasoned Judgment	17
39.	Identification of Specific Information	17
40.	Specific Classifying Criteria	18
41.	Presumption of Damage	18
42.	Prohibitions	18
43.	Classifying Scientific Research Data	19
44.	Classifying Documents	19
45.	Classifying Material Other Than Documents	20
46.	State-of-the-Art and Intelligence	20
47.	Effect of Open Publication	20
48.	Reevaluation of Classification Because of Compromise	20
49.	Compilation of Information	21
50.	Extracts of Information	21
51.	Classification Review of Produced Material	21
52-53.	RESERVED	22
SECTION 3.	DURATION OF ORIGINAL CLASSIFICATION	22
54.	General	22
55.	Duration of Classification	22
56.	Challenges to Classification	23
57.	RESERVED	24

TABLE OF CONTENTS

	<u>Page No.</u>
CHAPTER 1. GENERAL PROVISIONS	1
SECTION 1. INTRODUCTION	1
1. Purpose	1
2. Distribution	1
3. Cancellation	1
4. Explanation	1
5. Statement of Intent	2
6. Scope	2
7. Responsibilities	2
8. Authority to Originally Classify Information	3
9. Authority to Downgrade or Declassify	4
10. Administrative Sanctions	4
11. Interpretation	5
12. Maintenance of This Order	5
13. RESERVED	5
SECTION 2. DEFINITIONS	5
14. Definitions	5
15-20. RESERVED	10
SECTION 3. PROGRAM MANAGEMENT	10
21. General	10
22. FAA Classified Information Program Structure	10
23. Classified Account Custodians	11
24. Top Secret Control Officer (TSCO)	12
25. Account Audits	12
26. Security Inspection Report (RIS:CS 1600-26)	12
27. Supplementation	12
28-29. RESERVED	13 (and 14)

FOREWORD

This order provides direction, and assigns responsibility for assuring agency compliance with the provisions of Executive Order 12065, dated June 28, 1978.

The material in this order provides direction on the many aspects of the classified information security program as it is outlined by E.O. 12065. The only significant changes to the procedures utilized for several years in FAA have to do with the marking of classified documents, and the requirement for earlier declassification of most information.

The previous edition of this order contained a significant amount of material that did not relate specifically to the control and protection of national security information. In order to improve the quality of this directive, all nonrelevant information has been deleted. This material will be incorporated into other FAA security directives. Appropriate references to these directives are included in this order.



ALAN W. READ
Director of Investigations
and Security

CHAPTER 1. GENERAL PROVISIONS

SECTION 1. INTRODUCTION

1. PURPOSE. This order implements DOT Orders, 1640.3C, National Security Information, and 1640.4A, Classification, Declassification, and Control of National Security Information. It establishes comprehensive standards for the protection of classified national security information held, used or generated by FAA components. It also establishes a system for the classification, downgrading and declassification of information; sets forth policies and procedures for the safeguarding of such information; and provides a management control process for the FAA classified information security control program.

2. DISTRIBUTION. This order is distributed to branch level in the Office of Investigations and Security in headquarters; to branch level in the Air Transportation Security Division in the regions; to branch level in the Investigations and Security Division at the Aeronautical Center and to branch level in the Aviation Facilities Division at NAFEC.

3. CANCELLATION. Order 1600.2A, dated 13 February 1973, is canceled.

4. EXPLANATION OF CHANGES. Changes were made to include the provisions of Executive Order 12065. Essentially, these are:

a. The classification category "Confidential" has been redefined.

b. The types of information which qualify for classification are specified.

c. The period during which information may remain classified has been reduced to six years, except in certain cases.

d. Marking requirements are changed to require the identification of classified and unclassified portions of documents. Also, there are new provisions for the identification of a classification authority.

e. Procedures are established for the systematic review of classified information.

f. The Information Security Oversight Office replaces the Interagency Classification Review Committee.

g. Guidance and information superfluous to the purpose of this order have been deleted.

5. STATEMENT OF INTENT. It is the intention of the FAA to provide an appropriate level of protection for classified national security information by complying with the standards established in Executive Order 12065.

6. SCOPE.

a. The provisions of this order apply to all FAA personnel who handle or otherwise have access to classified information, regardless of location, duty station or position.

b. FAA personnel located on military bases, embassies or contractor facilities are governed by the provisions of this order. Problems in compliance which result from either conflicting policies or constraints imposed by the non-FAA authority having security cognizance for the facility, installation or activity where a FAA employee or organization element is located, shall be referred to the appropriate FAA servicing security element for resolution.

c. FAA procurement actions which result in the production of classified information or require the contractor to utilize such information in the performance of the contract, shall be accomplished in accordance with FAA Order 1600.56, Guidelines for FAA Participation in the Department of Defense (DOD) Industrial Security Program (ISP).

7. RESPONSIBILITIES.

a. The Director of Investigations and Security, ASE-1, is responsible for:

(1) Developing FAA wide policies and standards required to safeguard classified national security information.

(2) Assuring compliance throughout FAA with these policies and standards.

(3) Developing management plans, programs and techniques for the efficient, cost effective control, handling and protection of classified national security information.

(4) Conducting investigations in the event of a loss or compromise of classified information and/or violation of the administrative controls prescribed in this or other directives for the protection of classified national security information.

b. Directors of Regions, Aeronautical Center and NAFEC, are responsible for the implementation of this order within their areas of jurisdiction.

c. Heads of offices, services and activities are responsible for safeguarding classified information entrusted to their custody in accordance with these policies and procedures.

d. Each FAA employee is responsible for assuring that classified national security information is properly used and safeguarded and that the administrative controls prescribed by this order are followed.

8. AUTHORITY TO ORIGINALLY CLASSIFY INFORMATION. Executive Order 12065 confers upon the Secretary of Transportation the authority to originally classify information as Secret and Confidential with further authorization to delegate this authority. This authority has been delegated to FAA as follows:

a. Normal Conditions. Authority to originally classify information as Secret and Confidential is delegated to the:

- (1) Administrator, AOA-1.
- (2) Director of Investigations and Security, ASE-1.

b. Emergency Conditions. When Defense Readiness Condition Number Two (FAA Readiness Level Charlie) or higher emergency conditions may be declared, authority to originally classify information as Secret or Confidential is automatically delegated to the:

- (1) Deputy Administrator, ADA-1.
- (2) Regional and center directors.

c. Cancellation of Authority. The authority delegated under emergency conditions to the Deputy Administrator and regional and center directors is automatically cancelled when Defense Condition Number Three (FAA Readiness Level Bravo) or lower emergency level is declared.

d. Although the delegations of authority are expressed above in terms of positions, the authority is personal and is vested only in the individual occupying the position. The authority may not be exercised "by direction of" or "for" a designated official. The formal appointment or assignment of an individual to one of the identified positions or a designation in writing to act in the absence of one of these officials, however, conveys the authority to originally classify information.

9. AUTHORITY TO DOWNGRADE OR DECLASSIFY.

a. Originally Classified Material Original classification authorities, a successor in capacity or a supervisory official of either, a higher authority, and the Departmental Security Review Committee, are authorized to downgrade or declassify information originally classified by FAA. In addition, the Director of Investigations and Security, ASE-1, is authorized to downgrade or declassify information originally classified by an official within FAA and to resolve classification conflicts or doubts as to the appropriate classification of that information.

b. Derivatively Classified Material. The declassification authorities designated above and the Regional and Center security elements are authorized to declassify or downgrade derivatively classified material when such action does not conflict with classification decisions evidenced by the source material or instructions from the original classification authority.

10. ADMINISTRATIVE SANCTIONS.

a. Under the provisions of E.O. 12065, military and civilian employees of FAA are subject to administrative sanctions if they commit any of the following:

(1) Knowingly and willfully classify or continue the classification of information in violation of E.O. 12065, any implementing directive, or this order; or

(2) Knowingly, willfully and without authorization disclose information properly classified under E.O. 12065 or prior executive orders or compromise properly classified information through negligence; or

(3) Knowingly and willfully violate any other provision of E.O. 12065, any implementing directive, or this order.

b. Sanctions include a warning letter, formal reprimand, suspension without pay, forfeiture of pay, loss of security clearance, removal, termination of classification authority or other sanctions in accordance with applicable laws, and such action shall be taken against any officer or employee, regardless of position, responsible for a violation of this order.

c. Heads of offices, services, regions and centers shall assure that appropriate corrective action is taken whenever a violation occurs. The DSI Director of Investigations and Security shall be informed through ASE-1 when such violations occur.

11. INTERPRETATION. Questions on interpretation of the provisions of this order or their application shall be referred as appropriate to the servicing region/center or headquarters security element or to the Security Division, ASE-200.

12. MAINTENANCE OF THIS ORDER. This order is distributed by servicing security elements to individuals assigned responsibilities under this section and to activities having custody of classified information. The order shall be maintained in current form for ready reference by those individuals and activities.

13. RESERVED.

SECTION 2. DEFINITIONS

14. DEFINITIONS. The following definitions are provided for the terms used in this directive. As used in this order, the following terms and meanings shall be applicable.

a. Access, Accessibility. The ability and opportunity to obtain knowledge or possession of classified information. (An individual does not have access to information merely by being in a place where it is kept, provided the security measures in effect prevent him from gaining knowledge or possession of the information.)

b. Active Account. Classified documents held by a classified account custodian, which change periodically due to updating, addition or deletion.

c. Activity. An F.A activity is one or more elements which, when related by organizational responsibility and location, form an operating entity.

d. Alien. Any person not a citizen or national of the United States. (See immigrant alien and foreign national.)

e. Authorized Persons. Those persons who have a need-to-know for the classified information involved and who have been determined to be trustworthy by an official authorized to make such a determination.

f. Classification Authority. The authority vested in an official of the FAA to classify originally information or material that, pursuant to the provisions of this order, is determined by that official to require protection against unauthorized disclosure in the interest of national security.

g. Classification Guides. Guidance issued or approved by an original classification authority that identifies information or material to be protected from unauthorized disclosure and specifies the level and duration of classification assigned or assignable to such information or material under authority of Executive Order 12063. For purposes of this order, this term does not include DD Form 254, Contract Security Classification Specification.

h. Classified Information. Information or material that is: (1) owned by, produced for or by, or under the control of the United States Government, and (2) determined pursuant to Executive Order 12063 or prior orders and this directive to require protection against unauthorized disclosure, and (3) so designated.

i. Classifier. An individual who makes a classification determination and applies a security classification to information or material. A classifier may be an original classification authority or a person who derivatively assigns a security classification based on a properly classified source or a classification guide.

j. Classify. To determine that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made.

k. Clearance. A determination by an official and specified authority that an individual is considered trustworthy to have access to any and all classified information within a designated classification category for which he may have a need-to-know.

l. Communications Security (COMSEC). The protection resulting from any measures taken to: (1) deny unauthorized persons information related to national security that might be derived from telecommunications, or (2) to ensure the authenticity of such telecommunications.

m. Compromise. The disclosure of classified information to persons not authorized access thereto.

n. Custodian. An individual who has possession of or is otherwise charged with the responsibility for safeguarding or accounting for classified information.

o. Declassification. The determination that classified information no longer requires, in the interests of national security, any degree of protection against unauthorized

disclosure, together with a removal or cancellation of the classification designation.

p. Declassification Event. An event that eliminates the need for continued classification of information.

q. Derivative Classification. A determination that information is in substance the same as information that is currently classified, and a designation of the level of classification.

r. Document. Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, telegraphic messages, data processing cards and tapes, maps, charts, paintings, drawings, engravings, sketches, working notes and papers, reproductions of such things by any means or process, and sound, voice, magnetic or electronic recordings in any form.

s. Document Control Station. An office or activity which controls classified documents received from the Security Control Point. Normally the Document Control Station distributes these documents to sub-accounts within the office for operational purposes and for storage. All documents held by sub-accounts subordinate to a Document Control Station pass through the Document Control Station when being processed for transmittal or disposition.

t. Downgrade. A determination that classified information requires, in the interests of national security, a lower degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect such lower degree of protection.

u. Foreign Government Information. Information that is (1) provided to the United States by a foreign government or international organization of governments in the expectation, express or implied, that the information is to be kept in confidence; or (2) produced by the United States pursuant to a written joint arrangement with a foreign government or international organization of governments requiring that either the information or the arrangement, or both, be kept in confidence. Such a written joint arrangement may be evidenced by an exchange of letters, a memorandum of understanding, or other written record.

v. Foreign National. Any person not a citizen of, not a national of, nor an immigrant alien to, the United States. (A foreign national may not be granted a security clearance.) For purposes of security, foreign representatives as defined below are considered to be the same as foreign nationals.

w. Foreign Representative. A citizen or national of, or an immigrant alien to the United States who is acting as a representative, official, or employee of a foreign government, firm, corporation, or person.

x. Formerly Restricted Data. Information removed from the Restricted Data category upon a joint determination by the Department of Energy (or antecedent agencies) and the Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be adequately safeguarded as classified defense information. For purposes of foreign dissemination, however, such information is treated in the same manner as Restricted Data.

y. Immigrant Alien. Any person who has been lawfully admitted into the United States under an immigration visa for permanent residence. (Such individuals may be granted a security clearance, provided provisions of applicable personnel security regulations are followed.)

z. Information. Knowledge that can be communicated by any means.

aa. Information Security. The result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information the protection of which is authorized by executive order or statute.

ab. Marking. The physical act of indicating on material the assigned classification, changes in classification, and any special limitation on the dissemination of the information.

ac. Material. Any product or substance on, or in which, information is embodied.

ad. National Security. The national defense and foreign relations of the United States.

ae. National of the United States. A citizen of the United States, or a person who, although not a citizen of the United States, holds permanent allegiance to the United States.

af. Need-to-Know. NEED-TO-KNOW is the term given to the requirement that knowledge or possession of classified information shall be provided only to persons whose official duties or contractual obligations require such access. Responsibility for determining the NEED-TO-KNOW of a prospective recipient rests upon each individual who has possession, knowledge or control of the information. A prospective recipient may not make the determination. He may only justify this access.

ag. Official Information. Information which is owned by, produced for or by, or subject to the control of the United States Government.

ah. Original Classification. An initial determination that information requires, in the interest of national security, a specific degree of protection against unauthorized disclosure together with a designation signifying that such a determination has been made.

ai. Regrade. A determination that classified information requires a different degree of protection against unauthorized disclosure than currently provided, together with a change of classification designation that reflects such different degree of protection.

aj. Restricted Data. All data concerning (1) design, manufacture or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 142 of the Atomic Energy Act. (See also Section 11y, Atomic Energy Act of 1954, as amended.)

ak. Security Control Point. An individual or office having primary responsibility for receiving, controlling, disseminating, and disposing of classified documents received by an activity. All documents held by document control station and sub-accounts pass through the Security Control Point when being processed for transmittal or disposition.

al. Sensitive Compartmented Information. All information and material that requires special controls for restricted handling within compartmented intelligence systems and for which compartmentation is established.

am. Servicing Security Element. The headquarters, region, or center organizational element mentioned in paragraph 2 which is responsible for providing security services to a particular activity.

an. Short Title. An identifying combination of letters and numbers assigned to material for purposes of brevity.

ao. Special Access Program. Any program imposing "need-to-know" or access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information. Such a program includes, but is not limited to, special clearance, adjudication, or investigative requirements, special designation of officials authorized to determine "need-to-know", or special lists of persons determined to have a "need-to-know".

ap. Static Account. Classified documents held by a Classified Account Custodian, which do not change periodically due to updating, addition or deletion.

aq. Sub-Account. An office or activity which receives classified documents from either a Security Control Point or Document Control Station, for operational purposes. The sub-account is responsible for protecting the documents from unauthorized access and for transmitting or disposing of the documents through the controlling Security Control Point or Document Control Station.

ar. United States and Its Territories. The 50 States; the District of Columbia; the Commonwealth of Puerto Rico; the Territories of Guam, American Samoa, and the Virgin Islands; the Trust Territory of the Pacific Islands; the Canal Zone; and the Possessions, Midway, and Wake Islands.

as. Upgrade. A determination by competent authority that certain classified information requires, in the interests of national security, a higher degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect such higher degree.

15-20. RESERVED.

SECTION 3. PROGRAM MANAGEMENT

21. GENERAL. Executive Order 12065 obligates FAA to establish and maintain an active oversight program to ensure compliance with the provisions of the Executive Order. The requirements of this section are intended to fulfill this obligation.

22. FAA CLASSIFIED INFORMATION PROGRAM STRUCTURE

a. National Program Management. Chief, Security Division, ASE-200, serves as national program manager for the FAA classified information control program. This function will be accomplished through the following actions:

(1) Development of comprehensive policies and procedures required to implement the requirements of E.O. 12065.

(2) Collection and maintenance of program management statistics as required by Order 1600.58, Reports to the Interagency Classification Review Committee(ICRC).

(3) Performance of evaluations of region/center classified information control programs.

(4) Monitoring region/center compliance with the inspection and audit requirements of this order.

(5) Providing specialized guidance and assistance when requested by FIA components.

(6) Development of a comprehensive security education program.

b. Region/Center Program Management. The region/center security element having program management implementation responsibilities for the classified information control program shall accomplish this function through the following actions:

(1) Develop and maintain program management statistics required by Order 1600.58.

(2) Conduct the required inspection of classified information accounts as specified in paragraph 26.

(3) Assure that the semi-annual audits of Top Secret documents and annual audits of Secret and Confidential documents are accomplished in accordance with the requirements of paragraph 25.

(4) Provide guidance, assistance, and security educational material that may be required by region/center components.

23. CLASSIFIED ACCOUNT CUSTODIANS. The supervisor of each office/activity/facility or organizational unit having a classified information account will appoint in writing a Classified Account Custodian. This individual may be the operator of the Security Control Point or Document Control Station, and will be responsible for:

a. Assuring full compliance with the provisions of this order.

b. Developing and reporting to the servicing region/center security element the statistical data required by Order 1600.58.

c. Conducting annual audits of all classified documents. Conducting investigations into any known or suspected compromise of classified information or violations of security directives.

d. Reporting any known or suspected compromise of classified information or security directives to the servicing security element.

24. TOP SECRET CONTROL OFFICER (TSCO). Each activity having a requirement to handle Top Secret material shall appoint, in writing, A TSCO and an alternate TSCO. The TSCO, or alternate TSCO, may be the same individual as the operator of the Security Control Point. In any case, the TSCO, or alternate TSCO, shall receive and maintain the required accountability records and controls, dispatch all Top Secret material and conduct semi-annual audits.

25. ACCOUNT AUDITS. Comprehensive audits shall be conducted of all TOP SECRET, SECRET, and CONFIDENTIAL documents in accordance with the schedule outlined in this paragraph. Each audit shall consist of a visual comparison of the classified account control records with the documents on hand. Written certification of the completion of these audits shall be transmitted to the servicing security element. Any discrepancy in control records or indications of a missing document shall be reported verbally to the servicing security element immediately. Audits shall be conducted on the following schedules:

a. Top Secret. Audits by the TSCO or alternate TSCO shall be conducted semi-annually in June and December.

b. Secret and Confidential. Audits by custodians shall be conducted annually in December.

26. SECURITY INSPECTION REPORT (RIS:CS 1600-26). A security inspection of each classified account shall be performed by the servicing security element within the time frame specified in the following subparagraphs. An inspection will consist of a thorough examination of physical and administrative safeguards, and a random comparison of control records and classified documents. The size of the random sample will be consistent with the volume of classified material. Inspection results will be documented in a written inspection report that will be sent to the appropriate level of management of the inspected facility/office or activity. A copy of this report shall be sent to ASE-200.

a. Active Accounts. Each active account and sub-account shall be inspected annually by the servicing security element except that static accounts may be scheduled for biennial inspections.

27. SUPPLEMENTATION. This order may be supplemented by region and center security elements as necessary to provide additional internal instructions pertaining to the local situation. The

appendix method of supplementation as described in paragraph 4ld (1), Order 1320.1B, FAA Directives System, is recommended, as it provides the user with a cohesive body of organizational procedures and instructions.

28-29. RESERVED.

BLANK FRAME

FOR

PROPER PAGINATION

CHAPTER 2. CLASSIFICATION OF NATIONAL SECURITY
INFORMATION

SECTION 1. RULES GOVERNING CLASSIFICATION OF INFORMATION

30. PRINCIPAL. Except as provided in the Atomic Energy Act of 1954 as amended, Executive Order 12065 is the only basis for classifying national security information. Such information shall be classified in one of the three categories specified herein. If there is reasonable doubt which designation is appropriate, or whether the information should be classified at all, the less restrictive designation should be used or the information should not be classified.

31. CLASSIFICATION CATEGORIES. Official information which requires protection against unauthorized disclosure in the interest of the national security shall be classified in one of the following three categories:

a. Top Secret. This category shall be applied only to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

b. Secret. This category shall be applied only to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

c. Confidential. This category shall be applied only to information, the unauthorized disclosure of which reasonably could be expected to cause identifiable damage to the national security.

32. CLASSIFYING INFORMATION ONLY. It is emphasized that only information may be classified. Classified information requires protection regardless of the medium by which it is presented. It may be expressed orally, in written, photographic, or printed form, or embodied in equipment, on magnetic storage media, or other such material. Terms such as "classified document," "classified material," "classified letter," etc., are simply reference terms to describe items that contain or reveal classified information.

33. MATERIAL PRODUCED IN FAA CONTAINING CLASSIFIED INFORMATION.

a. Only those officials specified in paragraph 8 have authority to make original classification determinations. If an FAA employee not having classification authority generates information which is believed to warrant original classification, it shall be referred to the appropriate classification authority for determination. Pending a classification determination, all material containing this information, including that referred for determination, shall be marked with the recommended classification category and safeguard in accordance with the provisions of this order.

b. In most instances, classified information in FAA-produced material is based upon or otherwise reflects classification determinations made by an official outside the agency exercising original classification authority. In these instances, the FAA employee producing a document is not originally classifying the information contained therein when a classification marking is placed on the document. Rather, the FAA official is conforming to a previously reached classification determination.

34. ACCOUNTABILITY OF CLASSIFIERS. Classifiers are accountable for the appropriateness of the classifications they assign, whether by exercise of original classification authority or by derivative classification.

35. CLASSIFICATION APPROVAL.

a. When an official signs or finally approves a document or other material already marked to reflect a particular level of classification, he or she shall review the information contained therein to determine if the classification markings are appropriate. If, in his judgment, the classification markings are not supportable, he shall, at that time, cause such markings to be removed or changed as appropriate to reflect accurately the classification of the information involved.

b. A higher level official through or to whom a document or other material passes for signature or final approval becomes jointly responsible with the accountable classifier for the classification(s) assigned.

36. CLASSIFICATION PLANNING.

a. Advance classification planning is an essential part of the development of any plan, operation, program, research and development project, or procurement action that involves classified information. Classification aspects must be considered from the outset to assure adequate protection for the information and for the activity itself, and to eliminate

impediments to the execution or implementation of the plan, operations order, program, project, or procurement action.

b. A classification guide shall be developed by the responsible program office for each originally classified system, program, plan, or project as soon as practicable prior to the initial funding or implementation. Classification guides shall:

(1) Identify the information elements to be protected, using categorization to the extent necessary to ensure that the information involved can be identified readily and uniformly.

(2) State which of the classification designations (i.e., Secret or Confidential) applies to the information.

(3) State the duration of classification in terms of a period of time or future event.

(4) Either specifically indicate that the designations, time limits, markings, and other requirements of Executive Order 12065 are to be applied to information classified pursuant to the guide in accordance with this order or specify how they are to be applied.

c. Each classification guide shall be approved personally and in writing by an official specified in Paragraph 8 whose identity shall appear on the guide. Such approval constitutes an original classification decision.

37. RESERVED.

SECTION 2. CLASSIFICATION PRINCIPLES, CRITERIA, AND CONSIDERATIONS

38. REASONED JUDGMENT. Reasoned judgment shall be exercised in making classification decisions. A positive basis must exist for classification. Both advantages and disadvantages of classification must be weighed. If, after consideration of the provisions of this section of the order, there is reasonable doubt whether the information in question should be classified at all, the information shall not be classified.

39. IDENTIFICATION OF SPECIFIC INFORMATION. Before a classification determination is made, each item of information that may require protection shall be identified exactly. This requires identification of that specific information which comprises the basis for a particular national advantage or

advantages which, if compromised, would or could adversely affect the national security.

40. SPECIFIC CLASSIFYING CRITERIA. A determination to originally classify shall be made only by an authorized original classification authority and only when, first, the information is within the following categories and, second, the unauthorized disclosure of the information reasonably could be expected to cause at least identifiable damage to the national security. The determination involved in the first step is separate and distinct from that in the second. The fact that the information falls under one or more of the criteria shall not be presumed to mean that the information automatically meets the damage criteria. Information may not be considered for classification unless it concerns:

- a. military plans, weapons, or operations;
- b. foreign government information;
- c. intelligence activities, sources or methods;
- d. foreign relations or foreign activities of the United States;
- e. scientific, technological, or economic matters relating to the national security;
- f. United States Government programs for safeguarding nuclear materials or facilities; or
- g. other categories of information which are related to national security and which require protection against unauthorized disclosure as determined by the Secretary of Transportation. Recommendations concerning the need to designate additional categories of information that may be considered for classification shall be forwarded through channels to the Secretary for determination. Each such determination shall be reported promptly by ASE-1 to M-50 for reporting to the Director of the Information Security Oversight Office.

41. PRESUMPTION OF DAMAGE. Unauthorized disclosure of foreign government information or the identity of a confidential foreign source is presumed to cause at least identifiable damage to the national security.

42. PROHIBITIONS.

- a. Classification may not be used to conceal violations of law, inefficiency, or administrative error, to prevent

embarrassment to a person, organization or agency, or to restrain competition.

b. Basic scientific research information not clearly related to the national security may not be classified.

c. A product of non-government research and development that does not incorporate or reveal classified information to which the producer or developer was given prior access may not be classified until and unless the government acquires a proprietary interest in the product. This prohibition does not affect the provisions of the Patent Secrecy Act of 1952 (35 U.S.C. 181-188).

d. References to classified documents that do not disclose classified information may not be classified or used as a basis for classification.

e. Classification may not be used to limit dissemination of information that is not classifiable under the provisions of Executive Order 12065 and this order or to prevent or delay the public release of such information.

f. No document originated within FAA may be classified after receipt of a request for the document under the Freedom of Information Act or the Mandatory Review provisions of this order (section 1, chapter 3) unless such classification is consistent with this order and is authorized by the Secretary of Transportation.

g. Classification may not be restored to documents containing information already declassified and released to the public under this or prior directives.

h. A compilation of official public releases may not be classified.

43. CLASSIFYING SCIENTIFIC RESEARCH DATA. Ordinarily, except for information which meets the definition of Restricted Data, basic scientific research or results thereof shall not be classified. However, classification would be appropriate if the information concerns an unusually significant scientific "break-through" and there is sound reason to believe it is not known or within the state-of-the-art of other nations, and it supplies the United States with an advantage directly related to national security.

44. CLASSIFYING DOCUMENTS. Reference to a document is not a basis for classification unless the reference, standing alone, reveals classified information. The overall classification of a document, file folder, or group of physically-connected documents shall correspond to that of the most highly classified component.

The subject or title of a classified document should normally be unclassified. When the information revealed by a subject or title warrants classification, an unclassified short title shall be added for reference purposes.

45. CLASSIFYING MATERIAL OTHER THAN DOCUMENTS.

a. Items of equipment or other physical objects may be classified only when classified information may be derived from them by visual observation of their internal or external appearance or structure, or of an operation, test, application or use of such objects. The overall classification assigned to end items of equipment or objects shall be at least as high as the highest classification of any of its integrated parts.

b. If mere knowledge of the existence of the item of equipment or object would compromise or nullify its national security advantage, its existence would warrant classification.

46. STATE-OF-THE-ART AND INTELLIGENCE. Classification requires consideration of the information available from intelligence sources concerning the extent to which the same or similar information is known or is available to others. It is also important to consider whether it is known, publicly or internationally, that the United States has the information or even is interested in the subject matter. The state-of-the-art in other nations may often be a vital consideration.

47. EFFECT OF OPEN PUBLICATION. Appearance in the public domain of information currently classified or being considered for classification does not preclude initial or continued classification; however, such disclosures require immediate reevaluation of the information to determine whether the publication has so compromised the information that downgrading or declassification is warranted. Similar consideration must be given to related items of information in all programs, projects or items incorporating or pertaining to the compromised items of information. In these cases, if the release is shown to have been made or authorized by an official of the Executive Branch authorized to declassify and release such information, classification of clearly identified items shall no longer be continued. However, holders should continue classification until advised to the contrary by a competent Government authority.

48. REEVALUATION OF CLASSIFICATION BECAUSE OF COMPROMISE. Classified information, and information related thereto, that is or may have been compromised, shall be evaluated to determine whether it should remain classified. Upon learning that a compromise or probable compromise of specific classified information has occurred, the FAA employee involved shall contact the servicing security element for guidance.

49. COMPILATION OF INFORMATION. A compilation of unclassified items of information shall normally not be classified. In unusual circumstances, classification may be required if the combination of unclassified items of information provides an added factor which warrants classification under paragraph 40. Classification on this basis shall be used sparingly and shall be fully supported by a written explanation which will be provided with the material so classified. (See also paragraphs 41 and 42).

50. EXTRACTS OF INFORMATION. Information extracted from a classified source will be derivatively classified, or not classified, as the case may be, in accordance with the classification markings shown in the source. The overall marking and internal marking of the source should supply adequate classification guidance to the person making the extraction. If internal markings or classification guidance are not found in the source and no reference is made to an applicable classification guide that is available for use by the person making the extraction, the extracted information will be classified according to either the overall marking of the source, or guidance obtained from the classifier of the source material.

51. CLASSIFICATION REVIEW OF PRODUCED MATERIAL.

a. All classified material produced by FAA, whether original classification or derivative classification is involved, is subject to a classification review by the servicing security element. The security element should establish a means whereby this review can be accomplished routinely. The material shall be reviewed to determine whether or not it contains classified information and if classified information should not be contained in the material. The review shall ensure that:

- (1) the appropriate classification designation is assigned;
- (2) the downgrading/declassification markings are appropriate;
- (3) the proper markings are affixed to the overall document, to titles and subjects, and to individual pages and paragraphs;
- (4) the classifier, on original classification actions, is authorized to make the determination.

b. All classified documents produced within FAA shall be reviewed by security personnel concerned prior to transmittal from the headquarters, regional or inter office facility or when

such material produced by a subordinate element is received into the facility.

c. Exception to the pretransmittal security review is authorized for field activities which produce only a minimal number of classified documents and which do not have resident security personnel at the location; provided that the annual security inspection of the activity shall include appropriate review of all classified documents produced since the last inspection.

52-53. RESERVED.

SECTION 3. DURATION OF ORIGINAL CLASSIFICATION

54. GENERAL. At the time a determination is made by an official with authority to originally classify information as Secret or Confidential, a simultaneous decision must be made by that official as to the duration of time such classification must remain in force. In arriving at the classification duration, the classifier must exercise careful judgment as to how far in the future the basis for original classification will remain valid. Only in cases where a specific determination has been made that earlier declassification should not be accomplished, may original classification authorities specify declassification dates or events six years from the date of classification. In DOT only the Secretary of Transportation may make a decision to continue classification beyond six years.

55. DURATION OF CLASSIFICATION.

a. Information shall be classified only so long as its unauthorized disclosure would result in at least identifiable damage to the national security. Any willful extension beyond that period is a violation of Executive Order 12065.

b. Dates or events on which automatic declassification should occur shall be as early as possible consistent with the national security and, except as provided in paragraph c., below, shall be no more than six years from the date of the original classification. Any event specified for the determination of declassification shall be an event certain to occur in less than six years.

c. Classification may be prolonged for more than six years only when the Secretary of Transportation determines that the two conditions specified in paragraph 40 for original classification will continue throughout the entire period the classification

will be in effect, and only for one or more of the following reasons:

(1) The information is "foreign government information" as defined in this order;

(2) the continuing protection of the information is specifically required by statute;

(3) the continuing protection of the information is essential to the national security because it reveals intelligence sources or methods which, if lost, cannot be regained or replaced promptly;

(4) the continuing protection of the information is essential to the national security because it pertains to communications security;

(5) the information reveals vulnerability or capability data the unauthorized disclosure of which can reasonably be expected to result in nullifying the effectiveness of a system, installation or project important to the national security;

(6) the information concerns plans important to national security the unauthorized disclosure of which can reasonably be expected to result in nullifying the effectiveness of the plan itself or impeding its orderly implementation;

(7) the information concerns specific foreign relations matters the continued protection of which is essential to the national security or;

(8) Disclosure of the information would place a person in immediate jeopardy.

56. CHALLENGES TO CLASSIFICATION. If holders of classified information have substantial reason to believe that the information is classified improperly or unnecessarily or that an overly restrictive period for continued classification has been assigned, they are encouraged to discuss this problem with a representative of their servicing security element. The servicing security element shall seek resolution of the problem through coordination with the accountable classifier, whether or not the classifier is an FAA official or a member of another agency. When requested, anonymity of the challenger shall be maintained.

a. Challenges received concerning information classified in FAA shall be acted upon within thirty days of receipt by the accountable classifier. The challenger shall be notified of any changes made as a result of the challenge or the reasons why no

change is made. Such notice shall, in appropriate cases, advise the challenger that, within thirty days, the decision may be appealed to ASE-1.

b. Within thirty days after receipt of an appeal, ASE-1 may reverse, amend, or uphold the initial decision of the classifier, informing both the challenger and classifier of the determination made as well as the option of further appeal to the Departmental Security Review Committee, through M-50.

c. Pending final determination of a challenge to classification and appeal, the information or document in question shall be safeguarded as required for the level of classification initially assigned.

d. The fact that an FAA employee has issued a challenge to classification shall not, in any way, result in or serve as a basis for an adverse personnel action.

e. The provisions of this paragraph do not apply to or affect declassification review actions undertaken under the mandatory review requirements of section 1, chapter 3 of this order.

57. RESERVED.

SECTION 4. INDUSTRIAL OPERATIONS

58. CLASSIFICATION IN INDUSTRIAL OPERATIONS. Classification of information in private industrial operations shall be based only on guidance furnished by the Government. Industrial management may not make original classification determinations and must implement the classification decisions of the U.S. Government contracting authority. DD Form 254, "Contract Security Classification Specification," shall be used to convey contractual security classification guidance to industrial management. DD Forms 254 shall be changed by the originator to reflect changes in classification guidance and reviewed for currency and accuracy not less than once every year. Changes shall be in strict conformance with the provisions of Order 1600.56, Guidelines for FAA Participation in the Department of Defense (DOD) Industrial Security Program (ISP) and DOD 5220.22R, Industrial Security Regulation. Copies of these two directives shall be provided to all holders of the DD Form 254 as soon as possible. When no changes are made as a result of the annual review, the originator shall so notify all holders of the DD Form 254 in writing.

59. INDEPENDENT RESEARCH AND DEVELOPMENT.

a. Information in a document or material that is a product of Government-sponsored independent research and development conducted without access to classified information may not be classified unless the Government first acquires a proprietary interest in the product.

b. If no prior access was given but the person or company conducting the independent research or development believes that protection may be warranted in the interest of national security, the person or company should safeguard the information as if it were properly classified, and submit it to ASE-1 for evaluation. Upon receiving such a request for evaluation ASE-1 will make or obtain a determination whether a classification would be assigned if it were Government information. If the determination is negative, the originator shall be advised that the information is unclassified. If the determination is affirmative, the FAA shall make or obtain a determination whether a proprietary interest in the research and development will be acquired. If such an interest is acquired, the information shall be assigned proper classification. If no such interest is acquired, the originator shall be informed that there is no basis for classification and the tentative classification shall be cancelled.

60. OTHER PRIVATE INFORMATION. The procedure specified in paragraph 59 shall apply in cases such as an unsolicited contract bid, in which private information is submitted to an FAA element for a determination of classification.

61. RESERVED.

BLANK FRAME

FOR

PROPER PAGINATION

BLANK FRAME

FOR

PROPER PAGINATION

CHAPTER 5. ACCESS, DISSEMINATION, AND CONTROL OF
CLASSIFIED INFORMATION

SECTION 1. ACCESS

130. PRINCIPAL. Except as otherwise provided for this order no person may have access to classified information unless that person has been determined to be trustworthy and unless access is necessary for the performance of official duties.

a. A personnel security clearance is an indication that the trustworthiness decisions has been made. There shall be a demonstrable need for access to classified information before a request for a personnel security clearance can be initiated.

b. The number of people cleared and granted access to classified information shall be maintained at the minimum number that is consistent with operational requirements and needs. No one has a right to have access to classified information solely by virtue of rank or position.

c. The final responsibility for determining whether an individual's official duties require possession of or access to any element or item of classified information, and whether the individual has been granted the appropriate security clearance by proper authority, rests upon the individual who has authorized possession, knowledge, or control of the information and not upon the prospective recipient.

d. These principles are equally applicable if the prospective recipient is an organizational entity, including other Federal Agencies, Defense contractors, foreign governments, and others.

131. DETERMINATION OF TRUSTWORTHINESS. No person shall have access to classified information unless a determination has been made of that person's trustworthiness. This determination, referred to as a security clearance, shall be based on an investigation in accordance with Order 1600.1B, Personnel Security Program. Such clearance data is entered into, and is retrievable from the Personnel Management Information System (PMIS) by the servicing security element.

132. CONTINUOUS EVALUATION OF ELIGIBILITY. Supervisors shall continually evaluate information coming into their possession regarding persons granted security clearance to ensure the criteria cited in Order 1600.1B continue to be satisfied.

133. DETERMINATION OF NEED-TO-KNOW. In addition to a security clearance, an individual must have a need for access to the classified information or material sought in connection with the performance of official duties or contractual obligations.

134. REVOCATION OR RESCISSION OF SECURITY CLEARANCE.

a. Clearance revocation proceedings shall be referred thru ASE-1 to M-50 for a determination by the Secretary of Transportation in matters involving revocation.

b. A security clearance shall be administratively rescinded when an individual no longer requires access to classified information in the performance of official duties. Likewise, when an individual no longer needs access to a particular security classification category, the security clearance will be adjusted to the classification category still required for the performance of the individual's duties. In both instances, such action shall be taken without prejudice to the person's eligibility for security clearance should the need arise again. Order 1600.1B, sets forth policies, standards, procedures and designated authorities for the issuing and withdrawal of security clearances for FAA personnel.

135. ACCESS AND DISSEMINATION REQUIREMENTS IN GENERAL.

a. Access to certain types of information may require additional authorization and controls.

b. Supervisors are responsible for controlling the dissemination of classified information received or generated in their offices to persons under their jurisdiction.

c. Classified material originated by another department or agency and furnished to FAA shall not be distributed outside FAA without the prior consent of the originating department or agency. This restriction does not apply to additional distribution within the DOT or to distribution to contractors who require the information in performance of FAA contracts.

d. Classified material shall not be released to an employee or other person for his private use (personal, commercial, or as background material) even though the individual may have been partly or solely responsible for producing the material.

e. Before approving a release of classified information to a person who serves in more than one capacity, e.g., a contractor employee who also acts as a private consultant, the releasing official shall determine in which capacity the intended recipient is acting and will follow the release and clearance procedures established for the appropriate category.

f. Officials who disclose classified information verbally shall advise the recipients of the classification of the information divulged.

g. Additional provisions for dissemination in connection with visiting are set forth in chapter 9.

136. SPECIAL ACCESS PROGRAMS.

a. A Special Access Program is any program imposing "need-to-know" or access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information. Such a program includes, but is not limited to, special clearance, adjudication, or investigative requirements, special designation of officials authorized to determine "need to know", or special lists of persons determined to have a "need to know". The FAA is not authorized to establish a Special Access Program.

b. Participation by FAA employees in Special Access Programs established by other government agencies, shall be reported, in writing, through ASE-200 to M-50.

137-138. RESERVED.

SECTION 2. DISSEMINATION

139. DISSEMINATION WITHIN THE EXECUTIVE BRANCH. Classified information originated by DOT activities may be disseminated to other departments and agencies of the Executive Branch as necessary for the conduct of official business.

140. DISSEMINATION OUTSIDE THE EXECUTIVE BRANCH.

a. General. Classified information shall not be disseminated outside the Executive Branch without the specific authorization of ASE-1. Classified material which is to be released to U.S. entities outside the Executive Branch shall be marked to show that it shall not be further disseminated, in addition to other appropriate markings. Offices which release classified documents are responsible to assure that adequate physical safeguards will be provided by the receiving organization.

b. To the Congress.

(1) Provided other agency policies and procedures regarding legislative affairs are met, classified information may be disseminated to the Congress when necessary in the interests of the national security and as authorized by the Administrator.

As used herein, the Congress includes members, committees, subcommittees, and staffs of members and committees.

(2) Personnel who are to appear as a witness before a Congressional Committee or who will meet with staff representatives shall obtain prior approval from an authority designated above for the disclosure of classified information which he anticipates will be requested.

(3) A witness who is requested to disclose classified information which he has not been authorized to release shall respectfully state that he does not have authority to testify on the matter but that he will endeavor to obtain authority or have the information furnished.

(4) Witnesses shall request that classified testimony be given in executive session only, that any record of such testimony be identified as classified and not appear in any document subject to public inspection or availability, and shall obtain the assurance of a committee representative that everyone present has a security clearance commensurate to the classification of the information to be released.

(5) Personal communications to Congress shall not include classified information. Classified information shall not be furnished for further release to a constituent.

(6) Classified information to be disclosed shall be reviewed specifically to assure that the assigned classification is still valid.

c. To Representatives of the General Accounting Office (GAO). Properly cleared and identified representatives of the GAO may be granted access to DOT classified information at FAA activities when such information is relevant to the performance of their statutory responsibilities and duties in accordance with the following:

(1) The GAO will give advance notice to the heads of FAA activities to be visited. Each announcement of a planned visit will include the purpose of the visit, names of the representatives, and if access to classified information is anticipated a certification as to the level of clearance of each representative.

(2) The following GAO officials are authorized to certify security clearances: The Comptroller General, his Deputy, and Assistants; The General Counsel and Deputy General Counsel; The Director and Deputy Director, Office of Personnel Management; The Director and Deputy Director, Office of Policy; the Directors, Deputy Directors, Associate Directors, and Assistant Directors of

the following Divisions: General Government Resources and Economic Development, Resources and Economic Development, Manpower and Welfare, International, Transportation and Claims, Procurement and Systems Acquisition, Federal Personnel and Compensation, Logistics and Communications, Financial and General Management Studies; and Regional Managers.

(3) GAO personnel can be identified by special credential cards issued by the Comptroller General. Each card is serially numbered and bears the photograph and signature of the authorized holder.

(4) Requests for the following types of information will be forwarded by ASE-200 through M-50 to the Assistant for GAO Liaison, M-202, who shall consult with M-50 for determination of whether or not the information is relevant to the performance of the GAO's statutory responsibilities and for authorization for release or access:

(a) Top Secret information;

(b) Other sensitive classified information falling in the general areas of tactical operations, intelligence, and communications security;

(c) Classified information originated by another department or agency of the Executive Branch.

(5) When classified documents are furnished to GAO representatives, they shall be informed of the classified nature of the information and of the need for safeguarding it properly. In this connection, the Comptroller General has agreed to establish a security system at least equal to that prescribed by the Executive Branch.

d. To the Government Printing Office (GPO). Classified material, except Top Secret and similarly unique material, may be released to GPO plants, Washington and field, for reproduction when necessary as determined by FAA officials responsible for meeting printing and reproduction needs. The Public Printer has established policies and standards commensurate with those of the Executive Branch for the clearance of GPO personnel and for the safeguarding of classified information.

e. To the Judiciary. Every effort shall be taken to prevent the disclosure of classified information in proceedings before civil courts. If classified information becomes, or it appears that it might become involved, the matter will be referred immediately by ASE-200 through M-50 to the General Counsel, OST. The General Counsel in consultation with the Director of Investigations and Security, OST, will furnish advice and

guidance as appropriate to the circumstances of the given situation.

f. To Foreign Governments, Foreign Nationals, and International Organizations.

(1) The release of classified information to foreign nationals (orally, visually, or documentary form) requires special attention and controls. This paragraph deals only with the protection and controlled release of classified information. Other Departmental directives in the area of international relations should be consulted also. The term foreign national includes a U.S. citizen acting as a representative of a foreign government or firm.

(2) In rare instances, an FAA activity may wish to hire a foreign national as an employee. In this regard, the provisions of applicable directives and the Federal Personnel Manual will be followed. In addition, if access to classified information is involved, the activity or office shall submit a request through the servicing security element to ASE-200 for authorization together with necessary personnel security forms. The following requirements shall be fulfilled:

(a) The request shall identify precisely the classified information intended for release. ASE-200 will determine releasability of the information in the manner described below as though the information were to be released to the government of the country of which the individual is a national. Activities shall only permit access to that classified information for which authorization has been obtained. Procedural controls shall be established to effectively screen all information furnished to the foreign national employee.

(b) A Full Field Investigation shall be completed and evaluated before access is granted. Interim authorizations are not permitted. Since investigation overseas will be involved, delays in completing the investigation should be anticipated. If it is not possible to obtain full investigation coverage, authorization shall be denied. Upon completion and evaluation, a clearance will not be issued. Rather, a limited access authorization will be granted for access only to specifically identified information.

(3) In the case of a foreign national consultant or contractor requiring access to classified information, the provisions of Order 1600.56 apply.

(4) Except for the above, classified information as a matter of principle and policy is not made available to a foreign national as an individual but is disclosed to his government.

The foreign national receives the information in his capacity as an official or representative of his government. By this means, the parent government accepts responsibility for the clearance of the individual and for the protection of the information.

(a) Policies governing the disclosure of classified military information to foreign governments are formulated by the National Military Information Disclosure Policy Committee (NDPC). Releases of certain other classified information, including Restricted Data, intelligence, and communications security information, are made pursuant to policies established by the agency or interagency entity having cognizance of the information proposed for release. Often the determination of cognizance is difficult and involved and, in many cases, more than one department or agency may need to be consulted for approval.

(b) As a prerequisite for release, the FAA when proposing such release, must make a clear determination that the benefits to the U.S. outweigh the disadvantages of disclosure. The cognizant department or agency must concur in this determination.

(c) The foreign government proposed as a recipient of U.S. classified information must officially assure this government that the information will be used only for official purposes, will be afforded protection at least equal to our requirements, will not be released to any other person or nation without our express permission, and corporate or proprietary rights (if any) in the information will be respected.

(5) No release of classified information to a foreign national or foreign government may be made by an FAA activity without the express consent of ASE-1.

(6) Application for visits of foreign nationals to FAA activities, wherein access to classified information may be involved, shall be made to ASE-200 at least thirty days in advance of the proposed visit. In the case of a civilian or military representative of a foreign government application may be made by a civilian or military attache' of the mission of the country concerned. For all other foreign nationals (including U.S. citizens representing foreign interests), application shall be made by the Chief of Mission (ambassador, minister, etc.) of the country concerned. Applications shall contain the following information concerning the proposed visitor:

(a) name in full, grade, title, and position;

(b) nationality, date and place of birth (in case of a civilian, furnish passport number);

(c) employer or sponsor (if other than government making application);

(d) name and address of installation(s) to be visited;

(e) date, time, and duration of proposed visit;

(f) purpose of visit in detail, including estimated degree of access required;

(g) security clearance status of visitor with his own government;

(h) where known and appropriate, names of individuals to be visited; and

(i) a certification that the visitor has been subjected to a military and political screening and does not constitute a security risk to the United States, that the visit and visitor are officially sponsored by his government which has officially cleared him to receive information on the stated purpose, that responsibility for the security of the information obtained is officially accepted by his government, that all information obtained will be used for official purposes only and will not be released to any other person or nation without the express consent of the U.S. Government, and that corporate or proprietary rights involved, patented, or not, will be respected and protected.

(7) Requests for documentary release of classified information shall be processed generally in accordance with the procedures prescribed above. Documents containing classified information approved for release shall be delivered to ASE-200 for onward transmission by means appropriate to the circumstances.

(8) It is emphasized that these provisions apply to all situations wherein a foreign national may gain access to classified information in the custody of FAA. They apply to visits of FAA personnel to foreign countries, participants in exchange missions, conferences, meetings, symposia, etc. To avoid embarrassment, personnel should be careful to avoid firm invitations or commitments to foreign nationals which may involve access to classified information until the express consent for access is obtained. Other department or agency approval or sponsorship of a foreign national visit, sometimes referred to as a clearance, does not authorize access to classified information in the custody of FAA. Any proposed release of, or access to, classified information involving a foreign national, which is not

covered in these provisions shall be submitted to ASE-200 for handling on a case-by-case basis.

g. To Historical Researchers.

(1) Persons outside the Executive Branch who are engaged in historical research projects may have access to classified information provided that: (a) access to the information will be clearly consistent with the interests of national security, and (b) the person to be granted access is trustworthy.

(2) The provisions of this paragraph apply only to persons who are conducting historical research as private individuals or under private sponsorship and do not apply to research conducted under government contract or sponsorship. Further, the provisions are applicable only to situations where the classified information concerned, or any part of it, was originated in DOT or by DOT contractors or where the information, if originated elsewhere, is in the sole custody of DOT. If any person requests access to material originated in another agency or to information under the exclusive jurisdiction of the National Archives and Records Service, General Services Administration, he should be referred to the other agency or to the National Archives and Records Service.

(3) When a request for access to classified information for historical research is received, it will be referred to the servicing security element. The security element shall obtain from the applicant completed Standard Form 86 in triplicate, Investigation Data for Sensitive Position, and Standard Form 87, Fingerprint Chart; a statement in detail to justify access, including identification of the kind of information desired and the organization or organizations, if any, sponsoring the research; and a written statement (signed, dated, and witnessed) with respect to the following:

(a) That he will abide by regulations issued by FAA:

(1) to safeguard classified information; and

(2) to protect information which has been determined to be proprietary or privileged and is not eligible thereby for public dissemination.

(b) That he understands that any classified information which he receives affects the security of the U.S.

(c) That he acknowledges an obligation to safeguard classified information or privileged information of which he gains possession or knowledge as a result of his access to files of the Department.

(d) That he agrees not to reveal to any person or agency any classified information or privileged information obtained as a result of his access except as specifically authorized in writing by the FAA and further agrees that he shall not use the information for purposes other than that set forth in his application.

(e) That he agrees to authorize a review of his notes and manuscript for the sole purpose of determining that no classified information or material is contained therein.

(f) That he understands that failure to abide by conditions of this statement will constitute sufficient cause for canceling his access to classified information and for denying him any future access, and may subject him to criminal provisions of Federal law as referred to in this statement.

(g) That he is aware and fully understands that the provisions of Title 18, U.S. Code, Crimes and Criminal Procedures, and of the Internal Security Act of 1950, as amended, Title 50, U.S. Code, prescribe, under certain circumstances, criminal penalties for the unauthorized disclosure of information respecting the national security and for loss, destruction or compromise of such information.

(h) That this statement is made to the U.S. Government to enable it to exercise its responsibilities for the protection of information affecting the national security. That he understands that any material false statement which he makes knowingly and willfully will subject him to the penalties of Title 18, U.S. Code, Section 1001.

(4) The security element shall process the forms in the same manner as specified for a preappointment NAC for a critical-sensitive position. Upon receipt of the completed NAC, the security office, if warranted, may determine that access by the applicant to the information will be clearly consistent with the interests of national security and the person to be granted access is trustworthy. If deemed necessary, before making its determination, the office may conduct or request further investigation. Before access is denied in any case, the matter will be referred through ASE-1 to M-50 for review and submission to the Secretary for final determination.

(5) If access to Top Secret, intelligence, or communications security information is involved a full field investigation is required. However, this investigation shall not be requested until the matter has been referred through ASE-1 to the M-50 for determination as to adequacy of the justification and the consent of other agencies as required.

(6) When it is indicated that an applicant's research may extend to material originating in the records of another agency, approval must be obtained from the other agency prior to the grant of access.

(7) Approvals for access shall be valid for the duration of the current research project but no longer than two years from the date of issuance, unless renewed. If a subsequent request for similar access is made by the individual within one year from the date of completion of the current project, access may again be granted without obtaining a new NAC. If more than one year has elapsed, a new NAC must be obtained. The security element shall promptly advise ASE-200 of all approvals of access granted under these provisions.

(8) An applicant should be given access only to that classified information which is directly pertinent to his approved project. He may review files or records containing classified information only in offices under the control of DOT. Procedures should be established to identify classified material to which he is given access. He should be briefed on local procedures established to prevent unauthorized access to the classified material while in the custody, for the return of the material for secure storage at the end of the daily working period, and for the control of his notes until they have been reviewed. In addition to the security review of the applicant's manuscript, the manuscript will be reviewed by appropriate offices to assure that it is technically accurate insofar as material obtained from the agency is concerned and is consistent with the FAA's public release policies.

h. To Former Presidential Appointees. Persons who previously occupied policy-making positions to which they were appointed by the President may be granted access to classified information or material which they originated, reviewed, signed, or received while in public office, provided that:

(1) It is determined that such access is clearly consistent with the interests of national security; and

(2) the person agrees to safeguard the information, to authorize a review of his notes to assure that classified information is not contained therein, and that the classified information will not be further disseminated or published.

i. To Contractors. Classified information may be disclosed to DOT contractors, subcontractors, bidders, and grantees, and to contractors of other Government agencies, provided access to the information is necessary to the performance of the contract and required security clearances have been issued.

j. To National Defense Executive Reservists (NDERs). For the purpose of dissemination, members of the DOT NDER program are considered to be in the same category as employees. Classified information may be disclosed to DOT NDER's for which they have a need provided clearances have been issued pursuant to the provisions of Order 1600.1B. However, classified material shall not be physically released to the custody of NDERs except upon request to the Director of Emergency Transportation, OST, and in accordance with procedures established by the latter, after consultation with M-50.

k. To Others. Proposed releases of classified information to persons not categorized above shall be referred to ASE-200 for approval and determination of limitations on release, if any, and measures necessary to assure the trustworthiness of the proposed recipient. ASE-200 shall be consulted before any commitment to or understanding with the individual or entity has been made.

141. DISSEMINATION THROUGH MEETINGS. Activities which host or convene a classified conference, symposium, seminar, exhibit, or scientific and technical gathering (hereinafter referred to as a meeting) shall assure that security measures, appropriate to the circumstances, are taken. Requirements include, but are not limited to, the following:

a. All persons attending the meeting shall be properly authorized and have a need for the information. In this regard, all attendees may not have a need for all of the information to be presented, particularly at a meeting covering a wide range of topics. In such instances, the agenda should be drawn and the meeting conducted in a manner to provide for selective attendance.

b. Attendees shall be positively identified before being admitted to the meeting room.

c. Persons who present classified information shall be advised of any limitations on their presentations which may be necessary because of the level of clearance or need-to-know of certain members of the audience. The speaker is responsible also for seeking such guidance and for keeping his disclosures within the prescribed limits.

d. Notes, minutes, summaries, recordings, proceedings, reports, etc., on the classified portions of the meeting shall be safeguarded and controlled throughout the duration of the meeting. Such material, as appropriate, shall be forwarded to attendees by secure means at the conclusion of the meeting rather than being handcarried by them from the meeting site (except for local attendees).

e. Physical and technical security controls shall be established as appropriate to the classification and sensitivity of the information to be discussed. Because of the security hazards inherent in the use of any normally public meeting place for the presentation or discussion of classified information, classified meetings or classified sessions of a meeting shall, whenever possible, be held only on a U.S. Government installation or a cleared contractor facility. Exception to this provision may be approved by the servicing security element.

142. RESERVED.

SECTION 3. CONTROL OF CLASSIFIED INFORMATION

143. GENERAL. Through effective accounting procedures it is possible to trace the movement of classified material, identify persons afforded access, limit dissemination, retrieve documents promptly, detect the loss of material and prevent excessive production and reproduction of documents.

144. SECURITY CONTROL POINT. A Security Control Point, to be operated by appropriately cleared personnel, shall be established within each activity which has a requirement to handle classified material. All incoming and outgoing classified material shall be processed through the Security Control Point. The primary duties of the Security Control Point are:

- a. Maintaining accountability records.
- b. Assigning control numbers to each new item of classified material entered into the control system.
- c. Locating classified material to be returned to the originating activity when required.
- d. Verifying the clearance status of initial recipients of incoming classified material.
- e. Routing downgrading and/or declassification notices to the holders of the classified material involved.
- f. Receiving, unopened, all incoming registered and certified mail and inspecting that mail which contains classified material for evidence of tampering or damage.
- g. Matching the actual contents of an incoming package of classified material with the enclosed receipt.

CHAPTER 3. REGRADING CLASSIFIED INFORMATION

SECTION 1. GENERAL PROVISIONS

62. PRINCIPAL. Declassification of information shall be given emphasis comparable to that accorded classification. Information classified pursuant to Executive Order 12065 and prior orders shall be declassified as early as national security considerations permit. Decisions concerning declassification shall be based on the loss of sensitivity of the information with the passage of time or on the occurrence of an event which permits declassification. When information is reviewed for declassification, it shall be declassified unless the declassification authority designated pursuant to paragraph 9 determines that the information continues to meet the classification requirements prescribed in paragraph 40 despite the passage of time.

63. SYSTEMATIC REVIEW FOR DECLASSIFICATION. The Secretary of Transportation may prolong beyond twenty years classification of information over which DOT exercises classification jurisdiction. This authority may not be delegated.

a. Classified information constituting permanently valuable records of the Government, as defined by U.S.C. 2103, and information in the possession and control of the Archivist of the United States, will be systematically reviewed for declassification by the Archivist as it becomes 20 years old. The OST Director of Investigations and Security is designated as the liaison officer for the Department with the Archivist for this purpose.

b. The OST Director of Investigations and Security will assure that guidelines for the systematic review of 20 year old classified information under DOT jurisdiction are issued and maintained. Guidelines will be prepared in consultation with the Archivist of the United States and will be reviewed by the Information Security Oversight Office.

64. MANDATORY REVIEW FOR DECLASSIFICATION. Executive Order 12065 requires that procedures be established to handle requests by a member of the public, by a government employee, or by an agency, to declassify and release information. In order to be acted upon, a request needs to describe the information with sufficient particularity to permit the record to be identified and located. Requests for declassification under this mandatory review provision shall be acted upon within 60 days. After review, the record or any reasonably segregable portion thereof that no longer is in the interest of national security shall be

declassified and released unless withholding is otherwise warranted under applicable law.

a. Requests for classified records made under the Freedom of Information Act, as amended, are processed differently than requests made under the mandatory review provision.

b. An agency in possession of a classified document may not, in response to a request for the document made under the Freedom of Information Act or the mandatory review provision of E.O. 12065, refuse to confirm the existence or nonexistence of the document, except where such confirmation would itself be classified.

65. SUBMITTING AND HANDLING REQUESTS FOR MANDATORY REVIEW. The Director of Investigations and Security, M-50, Office of the Secretary of Transportation, 400 7th Street, S.W., Washington, D.C. 20590, has been designated as the office to whom a member of the public or another department or agency may submit a request for mandatory review of classified material produced by or under the primary cognizance of the Department of Transportation. Elements of the FAA which may receive a request directly shall immediately notify M-50 through the servicing security element and ASE-200.

66. CLASSIFICATION REVIEWS UNDER THE FREEDOM OF INFORMATION ACT.

a. Public Law (P.L.) 93-502 amended the Freedom of Information Act (Section 552, Title 5, United States Code (U.S.C.)). Of particular significance to the program for the classification and control of national security information are those amendments (1) which relate to requests for classified records, and (2) those which prescribe time limits for reply to requesters.

b. The Act authorizes the withholding of records from public availability which are "(A) specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive Order." Persons who have requested records from an agency under the provisions of the Act and whose requests have been denied may petition the courts to enjoin the agency from withholding the record and, in this event, the burden is on the agency to sustain its action. It is essential, therefore, that classified records which have been requested under the act be subjected to a thorough classification review to determine whether continued classification is justified under the provisions of E.O. 12065.

c. With respect to time limits, P.L. 93-502 basically requires an initial determination to be made within 10 working

days after receipt of a request. In case of an appeal from an initial denial, a determination on the appeal is to be made within 20 working days after receipt of the appeal. Except for unusual circumstances, failure to respond within the stated time limits means that a requester has exhausted his administrative remedies and may bring suit immediately. It is essential, therefore, that initial and final determinations be made and the requester so advised within the applicable time frames.

67. INITIAL CLASSIFICATION REVIEWS.

a. The office having responsibility to act upon a Freedom of Information (FOI) request shall, in the event the requested record is classified, consult immediately with the appropriate security element which shall effect a classification review.

b. If it is determined that the information in the record does not warrant continued classification, the record shall be declassified, the action office shall be so advised, and a determination of releasability shall be made without further reference to security considerations. The fact that a record had been classified at one time but is now declassified is not pertinent to a determination of releasability and the provisions of 49 C.F.R., Part 7, Subpart G, Section 7.63, "Records relating to matters that are required by Executive Order to be kept secret," do not apply. A copy of the declassification decision resulting from the classification review shall be forwarded to the Director of Investigations and Security, N-50 through ASE-1.

c. If the classification review indicates that the information warrants continued classification, the security element shall so advise the action office prior to the expiration of the time limit who shall notify the requester that the request has been denied, following the provisions of 49 C.F.R., Part 7, Subpart C, Section 7.21, "Initial Determination".

(1) If it appears that the classification review cannot be completed within the time limit due to unusual circumstances, the security element shall so advise the action office who shall either

(a) arrange for an extension of the time limit in accordance with internal directives implementing 49 C.F.R., Part 7, Subpart C, Section 7.25, "Extension of Time Limits", or

(b) notify the requester that the request has been denied.

(2) A copy of a notification of initial determination to deny based on classification of a record shall be forwarded immediately to

(a) the Administrator

(b) M-50 through ASE-200. Under the Freedom of Information Act, M-50 will immediately inform the Chairman of the Security Review Committee who shall assure that action which is appropriate to the circumstances is taken. If the reason for the request for review is not based on the Freedom of Information Act, the matter shall be referred to ASE-1.

68. REMARKING OF MATERIAL. Material which no longer warrants classification as determined by a classification review shall be declassified and so marked. Material which continues to warrant classification shall be marked to indicate that a review was conducted and the date. Whenever possible a date for declassification shall be established and the material and accountability records shall be so annotated.

69-71. RESERVED.

SECTION 2. DECLASSIFICATION OF TRANSFERRED

DOCUMENTS OR MATERIAL

72. MATERIAL OFFICIALLY TRANSFERRED. In the case of classified information or material transferred pursuant to statute or Executive Order from one department or agency to another in conjunction with a transfer of functions (not merely for storage purposes), as distinguished from transfers merely for purposes of storage, the receiving department or agency shall be deemed to be the original classifying authority over such material for purposes of downgrading and declassification.

73. MATERIAL NOT OFFICIALLY TRANSFERRED. When any FAA element has in its possession classified information or material originated in an agency outside the DOT that has ceased to exist and such information or material has not been transferred to another department or agency within the meaning of paragraph 72 or when it is impossible to identify the originating agency, the FAA shall be deemed to be the originating agency for the purpose of declassifying or downgrading such information or material.

a. If it appears probable that another department, agency, or DOT component may have a substantial interest in the classification of such information, the FAA element shall notify such other department, agency, or DOT component of the nature of the information or material and any intention to downgrade or declassify it.

b. Until sixty days after such notification, the FAA shall not declassify or downgrade such information or material without consulting the other department, agency or DOT component. During

such period, the other department, agency, or DOT component may express objections to downgrading or declassifying such information or material.

74. TRANSFER FOR STORAGE OR RETIREMENT. Classified documents shall be reviewed for downgrading or declassification before they are forwarded to a Records Center for storage or to the National Archives for permanent preservation. Any downgrading or declassification determination shall be indicated on each document by markings as required by chapter 4.

75. RESERVED.

SECTION 3. REGRADING

76. RAISING TO A HIGHER LEVEL OF CLASSIFICATION. The upgrading of classified information to a higher level than previously determined, by officials with appropriate classification authority and jurisdiction over the subject matter, is permitted only when all known holders of the information: (1) can be notified promptly of such action, and (2) are authorized access to the higher level of classification or the information can be retrieved from those not authorized access to information at the contemplated higher level of classification.

77. CLASSIFICATION OF INFORMATION PREVIOUSLY DETERMINED TO BE UNCLASSIFIED. Unclassified information, once communicated as such, may be classified only when the classifying authority: (1) makes the determination required for upgrading in paragraph 76; (2) determines that control of the information has not been lost by such communication and can still be prevented from being lost, and (3) in the case of information released to secondary distribution centers, such as the Defense Documentation Center, determines that no secondary distribution has been made and can still be prevented. All known holders of information that has been upgraded shall be notified promptly of the upgrading action.

78. DOWNGRADING. When it will serve a useful purpose, original classification authorities may, at the time of original classification, specify that downgrading of the assigned classification will occur on a specified date or upon the occurrence of a stated event.

79. RESERVED.

BLANK FRAME

FOR

PROPER PAGINATION

CHAPTER 4. MARKING OF CLASSIFIED
INFORMATION

SECTION 1. GENERAL

80. DESIGNATION OF CLASSIFIED INFORMATION. Information determined to require classification protection under the provisions of this order shall be so designated. Designation by physical marking serves to warn the holder about the classification of the information involved; to indicate the degree of protection against unauthorized disclosure that is required for that particular level of classification; and to facilitate downgrading and declassification actions.

81. MARKING OF DOCUMENTS IN GENERAL. Examples of markings described in this chapter are included in figures 2 through 4.

82. ORIGINAL CLASSIFICATION. The following shall be shown on the face of originally classified documents:

- a. The identity of the original classification authority.
 - b. The date of classification and office of origin.
 - c. The overall classification of the document.
 - d. The date or event for automatic declassification or for review for declassification.
 - e. Documents classified for more than six years shall also be marked with the identity of the classifier who authorized the prolonged classification and the reason(s) the protection requirement is expected to continue despite the passage of time.
- NOTE: In DOT, the Secretary is the only official authorized to extend classification beyond six years.

83. DERIVATIVE CLASSIFICATION. The following shall be shown on the face of derivatively classified documents:

- a. The source of classification, i.e., source document or classification guide.
- b. The FAA office of origin of the derivatively classified document.
- c. The overall classification of the document.

d. The declassification date or event, or the date established for review for declassification. These dates shall be carried forward from the classification source. If the classification is based on multiple sources, the date or event which will retain the classification the longest shall be used.

e. Any downgrading action to be taken and the date thereof.

84. SPECIAL NOTATIONS. In addition to the foregoing, any appropriate special marking on the source material shall be carried forward to the new document, e.g., Restricted Data or Formerly Restricted Data; Intelligence Sources and Methods Involved; dissemination and reproduction notices.

85. IDENTIFICATION OF CLASSIFICATION AUTHORITY. Identification of a classification authority shall be shown on the face, or by notices or other means in the case of non-written material, and shall be such that, standing alone, it is sufficient to identify a particular official, source document, or classification guide.

a. If all information in the document or other material is classified by an act of ORIGINAL classification, the classification authority shall be identified on the "Classified by" line.

b. In cases of DERIVATIVE classification, the "Classified by" line shall identify the official making the derivative decision, while the "Based on Line" shall identify the source document or classification guide, including its date.

c. If the classification of information contained in a document or material is derived from more than one document, classification guide, or combination thereof, the "Based on" line shall be marked "multiple sources" and identification of all such sources shall be maintained with the file or record copy.

86. RESERVED.

SECTION 2. SPECIFIED MARKING REQUIREMENTS

87. OVERALL AND PAGE MARKING. The overall classification of a document, whether or not permanently bound, or a copy or reproduction thereof, shall be conspicuously marked or stamped with the appropriate classification designation at the top and bottom of any title page or front and back covers, and on the first and last pages. Each interior page of a document shall be conspicuously marked or stamped at the top and bottom with the highest classification of the information on the particular page.

88. MAJOR COMPONENT MARKING. Major components of a classified document which may be used separately, such as appendices, attachments, annexes, enclosures, chapters, etc., shall be marked as individual documents.

89. PORTRION MARKING. Whenever a classified document contains either more than one level of security classification or unclassified information, each portion, section, paragraph or subparagraph shall be marked to show the level of classification or that it is unclassified. It is the intent of this requirement that all portions of a classified document be sufficiently marked so as to eliminate any doubt which portions contain classified information.

a. The parenthetical symbols "(TS)" for Top Secret, "(S)" for Secret, "(C)" for Confidential, and "(U)" for Unclassified shall be placed immediately preceeding the text it governs.

b. When appropriate, the symbols "(RD)" for Restricted Data and "(FRD)" for Formerly Restricted Data shall be added, e.g., "(S-RD)" or "(C-FRD)".

c. Portion marking for documents containing foreign government information shall be marked to reflect the country or international organization of origin as well as the appropriate classification, e.g., "(NATO-S)" or "(U.K.-C)".

d. If, in an exceptional situation, parenthetical portion marking is determined to be impracticable, the document shall contain a statement sufficient to identify the information that is classified and the level of classification. Thus, each portion of a classified document need not be separately marked if all portions are classified at the same level provided a statement to that effect is included in the document.

e. When elements of information in one portion require different classifications, but segregation into separate portions would destroy continuity or context, the highest classification required for any item shall be applied to the portion or paragraph.

f. Illustrations, photographs, figures, graphs, drawings, charts and similar portions of classified documents will be clearly marked to show their classified or unclassified status. Such markings shall not be abbreviated and shall be prominent and placed within or contiguous to the portion.

90. SUBJECTS AND TITLES. Subjects or Titles shall be marked with the appropriate symbol, "(TS)", "(S)", "(C)" or "(U)" placed immediately following and to the right of the item. When

applicable other appropriate symbols, e.g., "(RD)", and "(FRD)", shall be added.

91. UNCLASSIFIED MATERIAL. Wholly unclassified material shall not be marked except when it is necessary to clearly indicate that a decision has been made NOT to classify it. Normally, this would apply to pages containing unclassified information in a multipaged document.

92. RESERVED.

FIGURE 1. COMMONLY USED MARKINGS

At the time of origin, each classified document is marked on its face with one or more standard markings as follows:

1. Original Classification Not to Continue More than Six Years. The following markings are used with an original classification that will not continue beyond six years:

Classified by _____ (See Note 1)

Declassify on _____ (See Note 2)

Message Abbreviation:

DECL _____ (See Note 3)

2. Derivative Classification. The following markings are used with a derivative classification:

Classified by _____ (See Note 5)

Based On _____ (See Note 6)

or Declassify On _____ (See Note 7.a.)

Review On _____ (See Note 7.b.)

Message Abbreviations:

DECL _____ (See Note 3)

or

REF _____ (See Note 4)

3. Downgrading. The following marking is used to specify a downgrading:

Downgrade to _____ (See Note 8)

Message Abbreviations:

DS _____ (See Note 9)

4. The Restricted Data and Formerly Restricted Data markings are, in themselves, evidence of extended classification. Therefore, except for electronically transmitted messages, only a completed "classified by" line is added above each a marking.

2/5/80

FIGURE 1. COMMONLY USED MARKINGS (Cont'd)

Note 1: Insert identification of original classification authority.

This line may be omitted if the original classification authority is also the signer or approver of the document.

Note 2: Insert the specific date or an event certain to occur.

Note 3: Insert day, month, and year for declassification, e.g., "June 6, 1979" or an event certain to occur.

Note 4: Insert day, month, and year for declassification review, e.g., "June 6, 1979."

Note 5: Insert identity of the official making the derivative decision.

Note 6: Insert identity of the single security classification guide, source document, or other authority for the classification. If more than one such source is applicable, insert the words "multiple sources."

Note 7: Insert: a. The specific date or event for declassification (when multiple sources are used, the latest of the declassification dates applicable to any of the source material is applied to the new document); b. The date for declassification review, as indicated by the source security classification guide or other source document as appropriate (when multiple sources are used, the latest of the declassification review dates applicable to any of the source material is applied to the new document).


Note 8: Insert Secret or Confidential and specific date or event, e.g., "Downgrade to CONFIDENTIAL on July 6, 1981."

Note 9: Insert "S" or "C" to indicate the downgraded classification and specific date or event, e.g., "S/C June 6, 1981."

2/5/80


1600.2B

FIGURE 2. SAMPLE CLASSIFIED LETTER

DEPARTMENT OF TRANSPORTATION FEDERAL AVIATION ADMINISTRATION		SECRET
DATE: April 3, 1980	WASHINGTON, D.C. 20591	
TO: ASST-900		
SUBJECT: Preparation of Classified Correspondence (U)		
FROM: ASST-900		
TO: Chief, Air Transportation Security Division, ASST-700		
<p>(U) Use the same format as for unclassified correspondence. Mark for classification as illustrated herein. Markings in this letter show that the first portion of the first paragraph is unclassified, subparagraph b is Secret and that other portions of the letter are classified as follows:</p> <ul style="list-style-type: none">a. (C) Subject, the third and fourth paragraphs and the second subparagraph b under the second paragraph: Unclassified.b. (S) The second paragraph, first portion, and the following subparagraph a: Secret. <p>(S) Control numbers must be assigned to classified documents.</p> <ul style="list-style-type: none">a. (S) This is accomplished by taking the completed document and all copies to the Security Control Point.b. (U) Be sure that the typewriter ribbon used in producing the classified document is removed from the machine and properly stored or disposed of. <p>(U) See pertinent portions of this order for added markings required for certain material (e.g., Restricted Data, Foreign Information).</p> <p>(U) This letter is marked to show the use of derivative classification by an FAA employee. The subject and paragraph markings, and "Unclassified" and "Declassify On" information are taken from the originally classified document (AEC OPLAN 79-03).</p> <p>John J. Doe</p> <p>Classified By: <u>Alvin E. Jones, ASST-900</u> Based On: <u>DO NOT OPLAN 79-03</u> Declassify On: <u>January 1, 1992</u></p> <p>(This sample letter is unclassified)</p> <p>SECRET</p>		

2/5/80

**FIGURE 3. SAMPLE LETTER OF
TRANSMITTAL FOR A CLASSIFIED DOCUMENT**

<p>DEPARTMENT OF TRANSPORTATION FEDERAL AVIATION ADMINISTRATION</p> <p>DATE: April 3, 1980</p> <p>TO: ASST-900</p> <p>FROM: Letter of Transmittal for a Classified Document (U)</p> <p>RE: ASST-900</p> <p>TO: Chief, Air Transportation Security Division, ASST-700</p> <p>This letter illustrates requirements for preparing a letter used to transmit a classified document.</p> <p>At the top and bottom of the transmittal letter mark the highest classification of any information in the transmittal letter itself or in any of its enclosures. In addition, if the transmittal letter itself contains classified information apply paragraph markings as shown in Figure 2.</p> <p>If the transmittal letter is classified at a lower level than the enclosure(s), or is unclassified, so state. Do this by including a final paragraph (as in this sample), or by marking such as:</p> <p style="padding-left: 40px;">When Separated from the Enclosure(s) this letter is (Unclassified) (Downgraded to Confidential)</p> <p>Show the classification and number of classified enclosures.</p> <p>Do not put "Classified By," "Exempt On," or "Declassify On" instructions on unclassified transmittal letters.</p> <p>This letter is (Confidential) or (Unclassified) when separated from enclosure(s).</p> <p>JOHN J. DOE</p> <p>Enclosures</p> <ol style="list-style-type: none"> 1. Draft Safe Haven Airport Plan (S) (1 copy) 2. Draft Recovery Plan (C) (1 copy) 3. Draft Evacuation Plan (C) (1 copy) <p>(This sample letter is unclassified)</p>	<p>SECRET</p> <p>WASHINGTON, D.C. 20591</p> 
---	--

SECRET

2/5/80

1600.2B

FIGURE 4. SAMPLE CLASSIFIED MESSAGE

TELEGRAPHIC MESSAGE

NAME OF AGENCY FAA Security Division, ASE-900 Washington, D.C.		PRECEDENCE ACTION: ROUTINE INFO:	SECURITY CLASSIFICATION CONFIDENTIAL
ACCOUNTING CLASSIFICATION		DATE FORWARDED 10/1/79	TYPE OF MESSAGE <input checked="" type="checkbox"/> DIRECT <input type="checkbox"/> INFO <input type="checkbox"/> GENERAL-ADMIN
FOR INFORMATION CALL			
NAME John J. Doe		PHONE NUMBER 426-4677	
THIS SPACE FOR USE OF COMMUNICATIONS UNIT			
MESSAGE TO BE TRANSMITTED (Use double spacing and all capital letters)			
<p>TO:</p> <p>ORIGINATORS OF CLASSIFIED MSGS</p> <p>(U) REFERENCE NSC MSG OF JULY 7, 1979</p> <p>(C) MARK SECURITY CLASSIFICATION AT THE TOP & BOTTOM</p> <p>(U) EACH PARAGRAPH SHALL BE MARKED AS SHOWN HEREIN</p> <p>(C) MARKINGS MAY BE APPLIED BY AN AUTOMATED SYSTEM PROVIDED THEY ARE MADE CLEARLY DISTINGUISHABLE ON THE FACE OF THE DOCUMENT FROM THE PRINTED TEXT.</p> <p>(U) THE LAST LINE OF PARAGRAPH & ALL SHOW THE DECLASSIFICATION/DOWNGRADING MARKINGS AS APPROPRIATE, I.E. "DECLAS MONTH/DAY/YEAR," "DO/CLASSIFICATION/ MONTH-DAY-YEAR," OR "NEW MONTH/DAY/YEAR." NOTE THIS SAMPLE MESSAGE HAS BEEN STRUCTURED ON A DERIVATIVE CLASSIFICATION BASIS WHEREIN THE REFERENCED MESSAGE BEARS THE ORIGINAL CLASSIFICATION AND DECLASSIFICATION DETERMINATION.</p> <p>(U) THE "CLASSIFIED BY" LINE IS NOT REQUIRED ON THE OUTGOING MESSAGE; HOWEVER, THE SECOND COPY OF THE MESSAGE SHALL SHOW THE CLASSIFIER AND THE SOURCE DOCUMENT IF APPLICABLE.</p> <p>DECL 7/7/85</p> <p>(SECOND COPY NOTATION IS AS SHOWN BELOW)</p> <p>CLASSIFIED BY: John J. Doe, ASE-900 BASED ON: NSC Msg 123456 of July 7, 79 DECLASS ON JULY 7, 1985</p> <p>(THIS SAMPLE MESSAGE IS UNCLASSIFIED)</p>			
PAGE NO.		NO. OF PGS.	
		SECURITY CLASSIFICATION CONFIDENTIAL	

STANDARD FORM 64
 GPO: 1974-500-002
 U.S. GOVERNMENT PRINTING OFFICE: 1974-500-002

BLANK FRAME

FOR

PROPER PAGINATION

SECTION 3. MARKING MATERIAL OTHER THAN DOCUMENTS

93. GENERAL PROVISIONS. Classification and declassification instructions shall be conspicuously stamped, printed, written, painted, or affixed by means of a tag, sticker, decal or similar device, on classified material other than paper copies of documents, and on containers of such material, if possible. If such is not practicable, written notification of the instructions shall be furnished to recipients. The following procedures for marking various materials are not all inclusive and may be varied to meet operational requirements and the physical characteristics of the material. In all cases, however, the concepts elucidated in this paragraph shall apply.

94. TRANSMITTAL DOCUMENTS. A transmittal document shall be marked to show the highest classification of the information contained in the transmittal as well as the material enclosed.

a. If the transmittal itself does not contain classified information, it shall be marked or stamped with the appropriate classification at the top and bottom of the first page only. In addition, it shall be marked at the bottom substantially: "Unclassified Upon Removal of Attachment(s)".

b. If the transmittal itself contains classified information it shall be marked as prescribed for other documents. If removal of the transmitted material will change the overall classification of the transmittal document, it shall be marked substantially: "Downgraded to (Appropriate Classification) Upon Removal of Attachments".

95. ELECTRICALLY TRANSMITTED MESSAGES.

a. The record copy of a classified message shall be marked as required in this Section for other classified documents.

b. The first item of information in the text of a classified message shall be its overall classification. Portions shall be marked as prescribed herein for paper copies of documents.

c. Paper copies of electronically transmitted messages shall be marked at the top and bottom with the assigned classification. When such messages are printed by an automated system, classification markings may be applied by that system, provided they are clearly distinguishable from the printed text.

d. The originator of a classified message will be considered the accountable classifier; thus, a "Classified by" line is not necessary in the electronically transmitted message. The source

of derivative classification assigned shall be annotated on the record copy.

e. The last line of text of a classified electronically transmitted message shall show the date for automatic declassification or for review for declassification.

96. FILES. File folders, binders, envelopes, etc., containing classified documents shall be conspicuously marked according to the highest classification of any document included therein.

97. TRANSLATIONS. Translations of United States classified information into a language other than English shall be marked to show the United States as the country of origin, with the appropriate U.S. classification markings and the foreign language equivalent thereof. Conversely, translations of foreign classified information into English shall be marked with the name of the country of origin and the foreign and U.S. equivalent classifications (see appendix 1).

98. CHARTS, MAPS AND DRAWINGS. Charts, maps and drawings shall bear the appropriate classification marking under the legend, title block or scale, in such a manner as to differentiate between the classification assigned to the document as a whole and the classification assigned to the legend or title. The markings shall also be inscribed at the top and bottom of each such document. Where the customary method of folding or rolling these documents would cover the classification markings, additional markings shall be placed so as to be clearly visible when the document is folded or rolled.

99. PHOTOGRAPHS. Negatives and positives shall be marked with the appropriate classification markings and kept in envelopes or other containers bearing conspicuous classification markings. Roll negatives shall be marked at the beginning and end of each strip, and single negatives marked with the appropriate classification. Each photographic print shall be marked with the appropriate classification at the top and bottom of the face side and, where practicable, the center of the reverse side. Caution must be exercised when using self-processing film or paper to photograph or reproduce classified material, since the negative of the last exposure may remain in the camera. All component parts of the last exposure shall be removed and destroyed as classified waste, or the camera itself shall be protected as classified material.

100. TRANSPARENCIES AND SLIDES. The applicable classification markings shall be shown on each transparency or slide. Other applicable markings, when practicable, shall be shown on the border, holder, or frame.

101. MOTION PICTURE FILMS. Classified motion picture films shall be marked at the beginning and end of each reel by titles bearing the appropriate classification. Such markings shall be visible when projected on the screen. Reels shall be kept in cans or other containers bearing conspicuous classification markings.

102. RECORDINGS. Recordings, sound or electronic, shall contain at the beginning and end a statement of the assigned classification which will provide adequate assurance that any listener or recipient will know that classified information of a specified level is involved. The recording material and containers shall also be marked conspicuously.

103. ELECTRICAL MACHINE AND AUTOMATIC DATA PROCESSING TAPES. Electrical machine and automatic data processing (ADP) tapes shall bear external markings and internal notations sufficient to assure that any recipient of the tapes will know that classified information of a specific classification level is involved. The markings will also serve to alert recipients that the classified information within the tapes requires protection when produced by any medium; e.g., terminal displays, printouts, etc.

104. PAGES OF ADP LISTINGS. Classification markings on pages of listings produced by ADP equipment may be applied by the equipment, provided the markings are clearly distinguishable from the printed text on the face of the document. As a minimum, such listings shall be marked with the security classification on the first and last pages and on the front and back covers, if any, as prescribed in above.

105. DECKS OF ADP CARDS. A deck of classified ADP cards need not be marked individually but may be marked as one single classified document so long as they remain within the deck. A deck so marked shall be stored, transmitted, destroyed and otherwise handled in the manner described for other classified documents of the same classification. An additional card shall be added, however, to identify the contents of the deck and the highest classification involved. Cards removed for separate processing or use and not immediately returned to the deck after processing shall be protected to prevent compromise of any classified information contained therein. In these instances, the cards shall be marked individually as prescribed above for an individual ordinary document.

106-109. RESERVED.

SECTION 4. CLASSIFICATION AUTHORITY, DURATION AND

CHANGE MARKINGS

110. DECLASSIFICATION AND REGRADING MARKING PROCEDURES.

Whenever classified information is downgraded or declassified earlier than originally scheduled, or upgraded by competent authority, the material shall be marked promptly and conspicuously to indicate the change, the authority for the action, the date of the action and the identity of the person taking the action. In addition, except for upgrading, prior classification markings shall be canceled, if practicable, but in any event those on the first page, and the new classification markings, if any, shall be substituted. In cases where classified information is downgraded or declassified in accordance with the downgrading and declassification markings prescribed in Figure 1, such markings shall be a sufficient notation of the authority for such action.

111. APPLYING DERIVATIVE DECLASSIFICATION DATES.

a. New material that derives its classification from information classified on or after December 1, 1978, shall be marked with the declassification date, event, or date for review assigned to the source information.

b. New material that derives its classification from information classified prior to December 1, 1978, shall be treated as follows:

(1) If the source material bears a declassification date or event not more than 20 years from the date of origin, the date or event shall be carried forward to the new material;

(2) If the source material bears no declassification date or event, or bears an indeterminate date or event such as "Upon Notification by Originator", "Cannot Be Determined", "Impossible to Determine", etc., or is marked for declassification beyond 20 years from date of origin, the new material shall be marked with a date for review for declassification 20 years from the date of original classification of the source material; and

(3) If the source material is foreign government information bearing no date or event for declassification or is marked for declassification beyond 30 years from date of origin, the new material shall be marked for review for declassification at 30 years from the time the information was originated by the foreign government or international organization of governments, or acquired or classified by the FAA, whichever is earlier.

c. New material that derives its classification from a classification guide issued prior to December 1, 1978, that has not been updated to conform with this order shall be treated as follows:

(1) If the guide specifies a declassification date or event 20 years or less from the date of original classification, that date or event shall be applied to the new material.

(2) If the guide specifies a declassification date or event more than 20 years from the date of original classification, or no declassification date or event, or an indeterminate date or event as in subparagraph above, a date for review declassification at 20 years from the date of original classification shall be applied to the new material.

112. UPGRADING. When material is upgraded, the old classification markings shall be cancelled promptly and new markings conspicuously applied.

113. RESERVED.

SECTION 5. ADDITIONAL WARNING NOTICES

114. GENERAL PROVISIONS.

a. In addition to the marking requirements prescribed in this chapter, warning notices prescribed in this Section shall be prominently displayed on classified documents or materials, when applicable. In the case of documents, these warning notices shall be marked conspicuously on the outside of the front cover, or on the first page if there is no front cover.

b. When display of warning notices on other materials is not possible, their applicability to the information shall be included in the written notification of the assigned classification.

115. RESTRICTED DATA. Classified documents or material containing Restricted Data as defined in the Atomic Energy Act of 1954, as amended, shall be marked as follows:

"RESTRICTED DATA"

"This material contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions."

116. FORMERLY RESTRICTED DATA. Classified documents or material containing Formerly Restricted Data, as defined in Section 142.d, Atomic Energy Act of 1954, as amended, shall be marked as follows:

"FORMERLY RESTRICTED DATA"

"Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination. Section 144.b, Atomic Energy Act, 1954."

117. INTELLIGENCE SOURCES AND METHODS INFORMATION. Classified information or material involving intelligence sources and methods and subject to specific dissemination controls shall be marked with the following additional warning notice:

"WARNING NOTICE--Intelligence Sources and Methods Involved."

118. DISSEMINATION AND REPRODUCTION NOTICE. Classified information that is determined by an originator to be subject to special dissemination or reproduction limitations, or both, shall include, as applicable, a statement or statements on its cover sheet, first page or in the text, substantially as follows:

"Reproduction requires approval of originator or higher authority."

"Further dissemination only as directed by (Insert appropriate office or official) or higher authority."

119. OTHER NOTATIONS. Other notations of restrictions on reproduction, dissemination or extraction of classified information may be used as shown on source material.

120. RESERVED.

**SECTION 6. REMARKING MATERIAL CLASSIFIED UNDER
PREVIOUS EXECUTIVE ORDERS AND DIRECTIVES**

121. GENERAL. Documents and material already marked under Executive Order 11652, as amended, or predecessor Orders and directives shall be remarked in conformity with this Chapter when (1) information extracted from material so marked is to be conveyed; (2) the document or material itself is to be disseminated in any manner; (3) the document or material is reviewed for specific purposes or during the annual security inspection. Whenever remarking of such documents or material is

required, it shall be accomplished in accordance with this Section.

122. FOREIGN GOVERNMENT INFORMATION. Documents or material classified before December 1, 1978, that contain foreign government information shall be marked for review for declassification 30 years from the date of origin, e.g., "Review on (insert date)."

123. REMARKING DOCUMENTS OR MATERIAL MARKED "SUBJECT TO THE GENERAL DECLASSIFICATION SCHEDULE" OR "ADVANCED DECLASSIFICATION SCHEDULE". A document or material, classified prior to December 1, 1978, and marked for automatic declassification in accordance with the General Declassification Schedule (GDS) or an Advanced Declassification Schedule (ADS) under Executive Order 11652 need not be remarked. However, should notification be made to extend classification beyond the declassification date or event specified by the GDS or an ADS, the document or material shall be remarked appropriately.

124. REMARKING DOCUMENTS OR MATERIAL MARKED AS "EXEMPT FROM THE GDS" OR NOT MARKED WITH ANY DECLASSIFICATION INSTRUCTIONS. A document or material classified before December 1, 1978, and marked as exempt from the GDS under Executive Order 11652 with a date or event for declassification 20 years or less from the date of origin, shall not be remarked. However, if a document or material exempted from the GDS is marked with a declassification date in excess of 20 years from the date of origin or does not bear a specific declassification date or event, it shall be marked with a date for review for declassification at 20 years from the date of origin of the document, e.g., "Review on (insert date)."

125. REMARKING DOCUMENTS OR MATERIAL MARKED "GROUP 4".

a. Information classified under Executive Order 10501, as amended, that is contained in a document or material marked as Group 4 and is still so marked, was placed by Executive Order 11652 under the General Declassification Schedule and subject to automatic declassification thereunder as follows:

(1) All such information originally classified as Top Secret becomes declassified on December 31 of the tenth year from the year of origin.

(2) All such information originally classified as Secret becomes declassified on December 31 of the eighth year from the year of origin.

(3) All such information originally classified as Confidential becomes declassified on December 31 of the sixth year from the year of origin.

b. When such information is determined to have been automatically declassified under subparagraph a(1),(2),(3), above, remarking of a document or material is not necessary but old classification markings shall be cancelled on at least the first page. In cases where such information remains classified under subparagraph a(1),(2), or (3), a finite date for declassification shall be shown on a "declassify on" line, prior classification markings cancelled on at least the first page, and current classification designations substituted therefor. However, should notification be made to extend classification beyond the declassification date or event specified by the GDS, the document or material shall be remarked appropriately.

126. REMARKING DOCUMENTS OR MATERIAL MARKED "GROUP 1, 2 OR 3" OR NOT GROUP MARKED. Information classified before June 1, 1972, that is contained in a document or material marked as Group 1, 2 or 3 under Executive Order 10501 as amended, or not group marked, shall be remarked to show a date for review for declassification 20 years from the date of origin, e.g., "Review on (insert date)".

127. EARLIER DECLASSIFICATION. Nothing in this section shall be construed to preclude declassification under paragraph 62.

128-129. RESERVED.

h. Signing and returning to the sender receipts enclosed in classified transmittals.

i. Assuring that the appropriate secure methods of transmission (except telecommunications) is selected and that the material is properly prepared for transmission.

j. Assuring that receipts are obtained for TOP SECRET and SECRET material sent from or within the activity. CONFIDENTIAL material mailed from the activity may be covered by receipts at the option of the sender.

k. Destroying or arranging for the destruction of classified material.

145. RECORDS.

a. Accountability records (FAA Form 1600-35) shall be established and maintained at the Security Control Point when classified material is:

- (1) received at an activity;
- (2) generated, reproduced, or destroyed within an activity;
- (3) transferred from one office to another within an activity; or
- (4) dispatched outside of an activity on a permanent or temporary basis, including that material which is handcarried out of the activity and which is to be returned.

b. The records maintained at the Security Control Point will, as a minimum, reflect the following:

- (1) Date of receipt and date of origination.
- (2) Activity from which received or by which originated.
- (3) A brief, unclassified description of the material.
- (4) Classification of the material.
- (5) The date of any downgrading action, the date for declassification or the date for review for declassification. Records shall be maintained in such a manner as to immediately identify classified material as it becomes downgraded or declassified or when it is eligible for a review for declassification.

(6) Control number assigned.

(7) The office within the activity currently having custody of the individual items of classified material.

(8) Disposition and date thereof for all material destroyed, downgraded, declassified or dispatched outside of the activity.

c. DOT F 1600.4, Classified Material Record, must also be used in all TOP SECRET and SECRET document transactions to fulfill internal and external continuous receipting requirements.

d. Accountability records, FAA Form 1600-35 and DOT F 1600.4, for classified material will be retained for a minimum of four years after final disposition is completed. At the end of this period they may be destroyed.

e. Automation of control records is authorized. Such action must have the prior approval of ASE-200.

146. WORKING PAPERS.

a. Working papers are documents, including drafts, notes, photographs, etc., accumulated or created to assist in the formulation and preparation of a finished document. Working papers produced by an activity which contain classified information shall be:

(1) Dated when created.

(2) Marked with the highest classification of any information contained in the document.

(3) Marked with downgrading or declassification instructions.

(4) Protected in accordance with the classification assigned.

(5) Destroyed when they have served their purpose by the appropriate Security Control Point.

b. Working papers classified at the Secret and Confidential level may be released within an activity for review and coordination without processing through the Security Control Point provided:

(1) That the recipient has the appropriate clearance, need-to-know and proper storage capability.

(2) That for Secret working papers a receipt is prepared by the releasing office identifying the material and is signed by the recipient.

(3) That the material either is destroyed within 30 days or returned to the originator. Secret working papers retained by any office more than 30 days shall be entered into the accountability system by the activity's Security Control Point.

c. All Confidential and Secret working papers transmitted outside of an activity on a temporary or permanent basis shall be processed through the Security Control Point.

147. ADDITIONAL TOP SECRET CONTROLS.

a. The Top Secret Control Officer will affix a disclosure record (DOT F 1600.32) to each TOP SECRET document which will reflect the document title; the name of all individuals given access to the TOP SECRET information, including those to whom only oral disclosure is made; and the date(s) of such access.

b. The internal and external transfer of TOP SECRET material will be covered by a continuous receipt system, regardless of how brief the period of custody.

c. The original and all copies of TOP SECRET documents will be numbered in series. Distribution records, receipts and accountability records will list the copy number as part of the document identification.

148. MATERIAL WHICH IS HAND-CARRIED TO OR FROM AN ACTIVITY. Personnel of an activity who receive TOP SECRET, SECRET, and CONFIDENTIAL material direct from a visitor or who bring such material back to their office as a result of their visiting another activity shall immediately have the material processed by the Security Control Point. Similarly, personnel who wish to release classified material to an authorized visitor or to another activity as a result of their visiting shall process the material through the Security Control Point.

149. DOCUMENT CONTROL STATION. In larger activities, which handle a significant volume of classified material and where the Security Control Point serves many offices, each office which has or will have custody of classified material shall establish a Document Control Station. The Station may be established organizationally at the office, service, division or lower level dependent upon the circumstances. The Document Control Station will receive all TOP SECRET, SECRET, and CONFIDENTIAL material that flows in or out of the office. The Document Control Station will maintain a record or log of all TOP SECRET, SECRET, and CONFIDENTIAL material received in the office. The log will also

indicate the individual or section which has custody of the material. The Security Control Point will forward all classified material intended for an office only to its Document Control Station which will assure that only appropriately cleared persons within its office receive, handle, or store the material. The Security Control Point will maintain a record of the identity and clearance of each Document Control Station operator.

150. EXCEPTIONS FOR UNIQUE MATERIAL. Communications Security, Registered Publications System, Special Intelligence, Restricted Data, and similar unique material will be received and accounted for by the respective custodians appointed for these purposes who shall operate in conformity with the regulations prescribed for the particular type of information.

151. RESERVED.

BLANK FRAME

FOR

PROPER PAGINATION

CHAPTER 6. STORAGE AND SAFEKEEPING OF CLASSIFIED MATERIAL

SECTION 1. STORAGE AND STORAGE EQUIPMENT

152. USE OF STORAGE CONTAINERS. To maintain a storage program that is both economical and effective the following steps shall be taken:

a. Classified material shall be consolidated in the least number of containers consistent with efficient operations and access requirements.

b. Unclassified material should be removed from the containers to the maximum extent possible without reducing the integrity of the files.

c. Containers shall be located so that they are under the direct observation of the custodian during working hours.

d. The contents of the containers shall be reviewed periodically for the purpose of reducing the volume of material on hand.

153. TYPES OF CONTAINERS AUTHORIZED.

a. Classified material may be stored only in containers which meet Federal Specifications GSA-FSS-AA-F-357 b,c,d,e,f and subsequent revisions, or GSA-FSS-AA-F-358 b,c,d,e,f, and subsequent revisions, or GSS-AA-F-00364a and subsequent revisions.

b. TOP SECRET material shall be protected by the most secure means feasible. As a minimum, it may be stored in a container specified above.

c. Caster bases for security containers are prohibited.

d. Offices which need to store classified material such as charts, maps, etc., which because of the size or volume cannot be placed in an approved container shall consult with the servicing security element.

154. OTHER FACTORS. Containers provide no absolute protection since they can be penetrated. The time required to open a container varies with its type. The equipments described above as authorized for the storage of classified material represent minimum requirements. A determination whether adequate protection is being provided will depend on the volume, nature, and sensitivity of the material in relation to other factors such

as type of containers, overall conditions which exist, presence of guards, vault-type space, intrusion alarms, etc. Such determinations shall be made for each specific location by the servicing security element.

155. SUPERVISION OF STORAGE CONTAINERS.

a. A custodian and one or more alternates will be assigned responsibility for the security of each cabinet or vault in which classified material is stored. STORAGE CABINETS SHALL BE KEPT LOCKED WHEN NOT UNDER THE DIRECT SUPERVISION OF THE CUSTODIAN OR OTHER PERSONS AUTHORIZED ACCESS TO THE CONTENTS OF THE CABINET. The number of persons afforded access to the storage containers shall be kept to a minimum.

b. Additional duties of the assigned custodian are:

(1) Insuring that the containers are locked and checked at the close of the workday and when the area is unattended during the workdays.

(2) Verifying that classified material withdrawn for use during the day had been returned to storage.

(3) Insuring that persons requesting or taking classified documents from the containers have the appropriate clearance and need-to-know.

(4) Insuring that the combinations are changed as prescribed in this chapter.

156. IDENTITY OF STORAGE FACILITIES. Each storage container shall be assigned a number or symbol for identification purposes which shall be affixed by decal or plate in a conspicuous location on the outside of the container. Form DOT F 1600.6, Lock Combination Record, or equivalent, will also be prepared showing the location of each container within an activity, the level of classified material authorized to be stored therein, the combination, and the names of persons having knowledge of the combination to each container. One copy of this record shall be maintained by the security element serving the activity. The servicing security element shall be notified when a storage container is to be relocated.

157. CONTROL OF COMBINATIONS.

a. Changing of Combinations.

(1) Combinations will be changed:

a. At the time the container is received by the office which will use it

b. At least annually.

(c) When there is reason to believe that an unauthorized person may have learned the combination.

(d) When a person who knows the combination transfers (including inter-office transfers) or terminates.

(e) When the container is to be used to store material of a higher classification than the clearance level of one or more of the persons who know the current combination.

(2) Normally, the combination will be changed by the designated custodian or by a cleared person specifically assigned that function within the activity. Under no circumstances should an outside locksmith be brought in for this purpose.

b. Protection of Combinations. COMBINATIONS MUST BE AFFORDED THE SAME DEGREE OF PROTECTION AS THE HIGHEST CLASSIFICATION OF THE MATERIAL IN THE CONTAINERS.

(1) Combinations shall NOT be carried in wallets, written on calendar pads or otherwise concealed in the work area. Knowledge of or access to the combination of a container will be given only to those appropriately cleared persons who are authorized access to the classified information in the container and need it for operational efficiency.

(2) When a combination is changed in accordance with the schedule set forth above the superseded combination is automatically declassified and may be destroyed without benefit of a destruction certificate.

(3) To ensure positive locking a combination dial should be rotated at least four complete turns in either direction.

(4) In selecting combination numbers, multiples of five, simple ascending or descending numbers, double numbers, telephone or room numbers and births, anniversary or any other prominent dates in one's life should not be used.

c. Standard Supply Combination. When a storage container or padlock is returned to stock, the returning office will first change the combination to 50-25-50 for cabinets and containers with built-in locks or to 10-20-30 for padlocks. A tag shall be affixed to one of the handles of the cabinet or shackle of the padlock showing the standard combination used and organizational symbol of the returning office. These two combinations are

reserved for cabinets and padlocks in supply stockage and are prohibited for use in securing classified material. The security element serving the activity shall be notified when the cabinet is removed from use.

158. SPECIAL PRECAUTIONS.

a. Reversible cardboard CLOSED-OPEN signs (GSA Supply Number 9905-296-7021, or equivalent) shall be used as additional reminders on classified storage containers.

b. To preclude the possibility of image transfer, front-coated copy paper should not be stored next to classified documents, otherwise it should be separated from the classified printed matter by a sheet of nonsensitive paper.

c. A Safe Check Record form, DCT F 1600.33, or equivalent, shall be placed on each container for the purpose of assuring a record is made of each time the container is opened, closed, and double checked.

d. Prior to a storage container being returned to storage, a careful search shall be made inside, behind, and under all drawers to assure that classified material is not inadvertently left in the container.

159. LOCK-OUT. In the event a security container or vault door needs to be penetrated by force to overcome a lock-out, the following provisions shall be observed:

a. Cleared personnel shall be used, unless such personnel are not available and an urgent need exists for access to the unit.

b. If damage is restricted to the locking drawer, the entire drawer shall be replaced with a new unit, or

c. All drilled or damaged parts (dial ring, lock case, etc.) shall be replaced with new parts and the drilled area shall be filled with weld equal in hardness to the surrounding metal, ground flush, and dressed and painted to conceal the repaired area. A metal plug inserted into the hole is not acceptable.

d. A record shall be maintained by the servicing security element showing the identity of the cabinet, date, and nature of repair.

160. RESERVED.

SECTION 2. CUSTODY AND AREA CONTROLS

161. BASIC PROVISIONS. Certain controls are fundamental to maintaining proper custodian protection of classified material. The following basic requirements are listed even though some individual items may be restated in other chapters. THEY ARE NOT ALL INCLUSIVE. Additional measures as necessary under existing circumstances shall be taken to prevent unauthorized access to the information.

a. AN ACTIVITY OR OFFICE WHICH MAY RECEIVE A CLASSIFIED DOCUMENT AND WHICH HAS NO AUTHORIZED SECURE STORAGE CAPABILITY SHALL TAKE ACTION TO PROTECT THE DOCUMENT. Such action shall include returning the document, destroying it or arranging with another activity or office for secure storage. Under no circumstances shall it be left unattended or in an unauthorized storage container.

b. Classified material shall not be displayed or left in an office when persons authorized to receive it are not present.

c. When being used, classified documents shall be covered with a Cover Sheet, DOT F 1600.7, or equivalent. The Cover Sheet will remain on the document when it is transmitted within an activity. It shall be removed when it is transmitted outside an activity or when it is placed in a file folder. The Cover Sheet shall be placed on the outside of file folders containing classified material so that these folders will be properly identified, upon removal from storage.

d. Offices having custody of classified material shall establish a system of checks to assure that classified material is placed in secure storage containers at the end of the day or when the office is unattended by authorized persons during the workday and that the cabinets are locked.

e. Employees assigned to an office shall assure that visitors are not afforded access to classified material unless security clearance data has been verified and the "need-to-know" has been established.

f. Classified waste shall be kept separate from unclassified material and shall be safeguarded in the same manner as accountable documents until destroyed. Offices using burn baskets or other receptacles for classified waste are responsible for removing all material from them at the end of each day unless the container is located in a 24 hour operational area under the control of responsible cleared personnel. The material shall be protected until forwarded to the control point for destruction. That portion of carbon paper ribbon and similar forms of "one-

time" typewriter ribbon which contain classified information shall be removed from the typewriter at the end of the typing project or the working day and handled as classified waste. Cloth-type ribbon shall be removed from the typewriter at the end of the day and stored if that portion of the ribbon which contains classified information has been used fewer than two times.

g. Classified information shall not be discussed over the telephone or sent via unsecured telecommunications circuits.

h. Classified information shall not be discussed with unauthorized persons and shall not be discussed in public or other places where it may be heard by unauthorized persons.

i. Classified material may not be removed from an activity except for official transmission or for the purpose of attending a conference or meeting.

j. Persons handcarrying classified material shall keep it in their personal possession at all times.

k. Classified material may not be checked with baggage and it may not be left in such places as: locked or unlocked automobiles, hotel rooms, hotel safes, aircraft, train compartments, buses, private residences, public lockers, etc.

l. Classified material shall not be read, studied, displayed, or used in any manner in a public conveyance or place.

m. Persons who are authorized to handcarry classified material shall be instructed as to their responsibilities for protecting it and action to be taken in the event it is lost or stolen.

n. Separate cassette type ribbons shall be utilized for typing classified information to assure safeguarding data and facilities storage.

162. CARE DURING EMERGENCIES. In the event of a fire alarm or other emergency (natural disaster, civil disturbance, etc.) requiring evacuation of office spaces, classified material shall be placed in locked storage cabinets or safes. Persons who are away from their offices and have classified material in their possession at the time shall assure that such material is safeguarded. If it cannot be protected, it shall be burned or destroyed beyond recognition on instructions from proper authority. All activities shall prepare plans for the emergency protection and/or destruction of classified material. The location and identity of the material to be destroyed, authorizing official(s), priorities for destruction, personnel

responsible for destruction, and recommended place and method of destruction should be predetermined and appropriate personnel indoctrinated.

163. AREA CONTROLS.

a. General. Under certain circumstances special measures are necessary to control entry into an area containing classified information in order to protect the information from unauthorized disclosure. In this event, the area shall be considered a CLOSED AREA. Usually, controlled areas related to specific rooms or physical spaces within a building.

b. Closed Area. A room or other space containing classified information shall be considered to be a Closed Area when:

(1) An individual may have access to classified information, visually or audibly, simply by being in the room. (This includes areas where classified information is normally or frequently displayed, such as on charts, maps, drawings, photographs, etc.

(2) The space is used as a major repository for classified files or documents such as a Security Control Point.

(3) Classified documents are being produced by the graphic arts process.

(4) A telecommunications center or terminal area which processes classified information.

(5) Because of the nature of the operations, classified information may otherwise be subject to undetected compromise.

c. Admittance to a Closed Area. Admittance to a Closed Area shall be controlled to prevent entry by unauthorized persons. ADMITTANCE SHALL BE LIMITED TO PERSONNEL ASSIGNED TO THE AREA AND TO PERSONS WHO ARE AUTHORIZED ACCESS TO THE CLASSIFIED INFORMATION IN THE AREA. Janitorial personnel may be admitted provided they are escorted and the classified information is covered or otherwise protected from observation, disclosure, or removal.

d. Physical Features of a Closed Area. A Closed Area shall be separated from adjoining spaces by barriers which will prevent uncontrolled entry and deny visual access. Rooms used for classified conferences or symposia shall be accoustically treated or secured by other measures designed to prevent unauthorized disclosure of information.

e. Specific Area Control Measures. The type of specific measures needed to establish adequate controls shall be determined by the servicing security office in coordination with safety officials. ASE-200 should be contacted with respect to security equipment or systems which might have unique application to particular situations or conditions.

f. Posting of Closed Areas. Areas that are designated as a Closed Area shall be posted to indicate this restrictive designation. Signs containing the words: "CLOSED AREA - AUTHORIZED PERSONNEL ONLY" shall be used. Lettering shall be on a contrasting background discernable, if practical, from a distance of 50 feet.

164. RESERVED.

CHAPTER 7. REPRODUCTION, TRANSMISSION AND
DESTRUCTION OF CLASSIFIED MATERIAL

SECTION 1. REPRODUCTION

165. DISCUSSION. The number of copies of a classified document shall be limited severely to those actually required for the orderly transaction of Departmental business. NO MORE COPIES THAN ACTUALLY NEEDED SHOULD EVER BE MADE. Holding the number of copies to the required minimum will decrease the risk of compromise of the information as well as the administrative burden in handling and protecting the documents.

166. AUTHORIZATION. Two types of authorization to reproduce material are involved:

(a) Authorization of the office which originated the document may be required, and (b) local authorization, which is required in EVERY INSTANCE.

a. Authorization of Originating Office.

(1) Those portions of classified documents which contain TOP SECRET information may not be reproduced without the express consent of the originating office or higher authority within the same organization. SECRET and CONFIDENTIAL documents may be reproduced unless the document itself contains a specific prohibition regarding its reproduction.

(2) The office having a requirement for additional copies is primarily responsible for obtaining such consent and shall maintain a record showing the consent.

b. Local Authorization.

(1) Supervisory personnel shall determine the need for additional copies and are responsible to hold to a minimum the number of copies required.

(2) Authorization of the Security Control Point or Top Secret Control Office shall be obtained to assure the prescribed accountability records are maintained for TOP SECRET, SECRET, and CONFIDENTIAL material.

167. ACCOUNTABILITY FOR REPRODUCED COPIES. Reproduced copies of all classified material shall be entered immediately into the accountability system. In addition, a DOT F 1600.32 shall be affixed to all TOP SECRET material.

168. MARKINGS. Classification and other security markings which appear on the document being reproduced shall appear on the reproduced copies. If the security markings do not show distinctly on the copies after reproduction has been completed, the copies SHALL BE REMARKED.

169. CONTROLS OVER REPRODUCTION EQUIPMENT AND AREAS. Reproduction equipment and areas normally fall within two categories: (a) Office copiers and (b) Printing and Photographic processes.

a. Office Copiers.

(1) Personnel shall exercise care in using office copiers to reproduce classified documents in order to prevent the information from being compromised. The following conditions represent SECURITY HAZARDS:

- (a) Leaving documents under the cover of flatbed exposure units.
- (b) Not realizing the last copy has not yet emerged from the delivery slot.
- (c) Ease by which other persons in the vicinity of the machine can read or take a copy.
- (d) Failure of the machine to deliver the number of copies mechanically ordered.
- (e) Damaged copies remaining inside the machine.
- (f) Failure to stay with the copier until service can be obtained in the event of a copier malfunction.
- (g) Failure to properly dispose of classified pages or classified waste.
- (h) Failure to destroy negatives or materials when using diffusion transfer or dry transfer machines.
- (i) Front-coated copy page transferring an image to the carrier belt inside certain single copy duplication machines or producing a "ghost" image on the next reproduced copy if a screen carrier is used.
- (j) Failure to use only Type 1 (back coated) thermal copy paper when reproduction is done by the thermal copy process.
- (k) Failure to handle as classified waste slip sheets which are placed between the film sheets in the diazo process.

(2) Facilities shall locate office copier used to reproduce classified documents in areas or in such a manner as to maximize the protection the operator can give to the material being reproduced. Facilities shall prepare guidance media, tailored to each type of office copier in the facility, to identify specific security hazards associated with each device and to assist operators in following secure practices when reproducing classified material. Such guidance, together with authorization requirements, shall be posted near copiers which are used by more than one office in the facility.

b. Printing and Photographic Process.

(1) Pressrooms, darkrooms, composition, bindery and proofreading rooms (or appropriate portions thereof) shall be regarded and designated a "Closed Area" when a classified production is in process. Admittance to the area will be limited to persons who have the requisite security clearance and whose presence in the area is required. During the printing stages of a classified run, presses will be identified to indicate the classification level of the work. The press shall remain so identified until the run is completed and all traces of classified information are removed; i.e., removal of the plates, blankets, chases, etc., from the press and the cleaning of the rollers and surfaces which may carry an impression.

(2) All material used in production that contains classified information (e.g., negative flats, layouts, master, drums, vellums, stencils, composition tapes, proofs, tympan sheets, negatives, type, plates, etc.) will be properly safeguarded and, if not destroyed as classified waste, entered into the accountability system. Plates and rubber blankets used on a classified production may be reused only on other classified jobs. Between runs they will be stored in approved security containers and be marked to indicate the highest category of classified information for which they were used.

170. RESERVED.

SECTION 2. TRANSMISSION OF CLASSIFIED MATERIAL

171. PREPARATION AND PACKING REQUIREMENTS (MAILABLE MATERIAL).

a. The following requirements apply to all classified material for transmittal outside an activity; however, TOP SECRET material shall not be mailed.

(1) Classified material shall be packaged in opaque inner and outer sealed envelopes, wrappings, or cartons.

(2) The inner cover shall be marked to indicate the highest classification of the material contained and other warning notations as appropriate. The outer cover shall have no classification markings or any other indication that classified information is enclosed. Markings on the inner cover shall not show through the outer cover.

(3) The inner and outer covers shall be addressed to the official government activity or cleared contractor and not to an individual. An attention line reflecting the internal routing symbol or organizational component within the receiving facility may be used on the inner envelope only.

(4) The receipt (optional for confidential material) shall be attached to or enclosed in the inner cover and shall identify the sending activity, addressee and the material being transmitted. The receipt shall contain no classified information. It shall be signed by the receiving activity and promptly returned to the sending activity.

(5) Material used for packaging shall be of such strength and durability so as to provide protection in transit and to prevent items from breaking out of the covers. Bulky packages shall be sealed with kraft tape laminated with asphalt and containing rayon fibers (snake tape) or nylon sensitive tape, or equivalent. Package shall be inspected prior to release to assure that they have been prepared properly for shipment.

b. The following requirements apply to all classified material for transmittal inside an activity, however, the activity's regular mail and messenger service shall not be used for TOP SECRET material.

(1) From one building to another requiring travel upon a public street or road, the material shall be prepared for transmittal in accordance with paragraph 167a above, except that a briefcase may suffice for an outer cover.

(2) For handcarrying within the same building by other than the mail or messenger system provide sufficient covering to prevent inadvertent disclosure of the classified information; e.g., a classified cover sheet.

(3) When the activity's regular mail and messenger system is used to deliver SECRET and CONFIDENTIAL documents, the material will be placed in a single sealed envelope with the classification stamped on the envelope. Cleared messengers only will be used.

(4) When an office having custody of classified material physically moves within a building or from one local building to

another, the material shall be retained in the locked safe-file normally used for classified storage or the material shall be securely packaged. In either instance, the custodian or other cleared personnel shall accompany the material and supervise the move. The servicing security element shall be notified prior to moving a safe containing classified material.

172. PREPARATION AND PACKAGING REQUIREMENTS (NON-MAILABLE BULK ITEMS).

a. If the classified material is an internal component of a packageable item of equipment whose outside shell or body is not classified and completely shields the classified aspects of the item from view, the shell or body may be considered as the inner covering.

b. If the classified material is an inaccessible internal component of a bulky item of equipment that is not reasonably packageable, the outside shell or body of the item may be considered as the outer covering provided the shell or body is not classified.

c. If the classified material is not reasonably packageable and the shell or body is classified, drape it with an opaque covering that will conceal all of the classified features and secure the covering in such a manner as to prevent inadvertent exposure of the item.

d. Specialized shipping containers, including closed cargo transporters, may be used in lieu of the packaging requirements listed above and are considered the outer wrapping or cover.

e. The assigned classification and the address of the consignee shall appear on or be attached to the inner covering, if one is used. The outer covering shall bear the address of both the cosignor and consignee. Under no circumstances will the outer covering or the shipping document attached to the outer covering reflect the classification of the contents or the fact that the contents are classified.

f. Containers shall be inspected prior to release to assure that they have been constructed, strapped, and otherwise prepared, including the use of seals when appropriate, to provide necessary protection during shipment.

173. METHODS OF TRANSMISSION.

a. Top Secret. The transmission of TOP SECRET information shall be effected preferably by oral discussion in person between the officials concerned. Otherwise, TOP SECRET information or material shall be transmitted by:

1 Personnel authorized access to the information or personnel specifically cleared and designated as a courier for this purpose. The normal mail and messenger system of an activity SHALL NOT BE USED. Postal services and commercial delivery services SHALL NOT BE USED.

(2) Armed Forces Courier Services (ARFCOS).

(3) Accompanied State Department diplomatic pouch.

(4) Telecommunications specifically approved by appropriate communications security authority for transmission of TOP SECRET Information.

b. Secret.

(1) Any means authorized for the transmission of TOP SECRET information. (Certain limitations are imposed on the use of ARFCOS for other than TOP SECRET material.)

(2) Appropriately cleared personnel.

(3) United States Postal Service registered mail within and between the Fifty States, District of Columbia, and Puerto Rico, provided the material does not at any time pass out of United States Government control.

(4) United States or Canadian registered mail with registered mail receipt for transmittal between United States Government and Canadian Government installations within the United States and Canada.

(5) United States Army, Navy, Air Force postal system under conditions established by the Department of Defense.

(6) Qualified carriers authorized to transport SECRET material via a Protective Security Service (PSS) under the Department of Defense Industrial Security Program. This method is authorized only for shipments within the United States and only when the size, bulk, weight, and nature of the shipment or escort considerations make the use of other methods impractical.

(7) United States Government carriers under escort of appropriately cleared personnel. Carriers included are Government vehicles, aircraft, ships of the United States fleet or civil service manned United States Naval ships. Appropriately cleared operators of vehicles, officers of ships or pilots of aircraft who are United States citizens may be designated as escorts provided the control and surveillance of the carrier is maintained on a 24-hour basis. The escort shall protect the shipment at all times, through personal observation or authorized

storage to prevent inspection, tampering, pilferage or unauthorized access until delivery to the consignee. However, observation of the shipment is not required during the period it is stored in an aircraft or ship in connection with flight or sea transit, provided the shipment is loaded into a compartment which is not accessible to any unauthorized persons aboard, or loaded in specialized shipping containers, including closed cargo containers.

(8) Telecommunications specifically approved by appropriate communications security authority for transmission of SECRET information.

c. Confidential.

(1) Any means approved for the transmission of SECRET material.

(2) United States Postal Service certified mail shall be used to mail Confidential material to U.S. Government activities and U.S. Contractors except that registered mail shall be used for CONFIDENTIAL NATO AND CENTO material and for FPO and APO addressees.

(3) Within United States boundaries, commercial carriers which provide a Security Signature Service (SSS) under the Department of Defense Industrial Security Program.

(4) In the custody of commanders or masters of ships of United States registry who are United States citizens. CONFIDENTIAL material shipped on ships of U.S. registry may not pass out of U.S. Government control. The commanders or masters must receipt for the cargo and agree to (a) deny access to the CONFIDENTIAL material by unauthorized persons, including customs inspectors, with the understanding that CONFIDENTIAL cargo which would be subject to customs inspection will not be unloaded and (b) maintain control of the cargo until a receipt is obtained from an authorized representative of the consignee.

174. ADVANCE NOTICE AND BILLS OF LADING.

a. To insure that classified material is properly received and protected upon delivery, the activity shipping bulk classified material by Government or commercial carrier will notify the consignee (including a military trans-shipping activity) in advance of the date of arrival, of the (1) nature of the shipment, (2) anticipated time and date of delivery, (3) means of shipment, and (4) number of seals if used. The consignee should also be requested to notify the consignor of any shipment not received within two working days after the estimated

time of arrival. Upon receiving such a notice, the consignor shall immediately request the carrier to trace the shipment.

b. Annotate the bills of lading to require the carrier to notify the cosignor immediately if the shipment is delayed en route. Bills of lading or other shipping documents shall NOT indicate that the shipment is classified.

c. Bulk material weighing less than 200 pounds gross shall be shipped only in a closed vehicle.

175. USE OF TELECOMMUNICATIONS. Classified information shall not be transmitted to points within or outside an activity. by telecommunications (e.g. telephone, teletype, data, radio, facsimilie, etc.) except by means which have been specifically approved by ASE-1.

176. ADDITIONAL REQUIREMENTS IN CONNECTION WITH VISITING.

a. Except for local visiting, if an employee has a need to have selected classified material in the custody of his office available to him at the place he will visit and THAT ACTIVITY DOES NOT HOLD COPIES OF THE MATERIAL, the material shall be forwarded to the activity to be visited with a notation on the inner envelope that it be held for the arrival of the named employee.

b. An exception to the above requirement may be made only under the most extreme circumstances when the visit and the need for the material could not be anticipated sufficiently in time to permit forwarding the material. In this event, the following provisions apply:

(1) Only those portions of a classified document which are essential for the visit shall be taken.

(2) A list itemizing the material to be taken shall be prepared, one copy to be retained by the security control point or the employee's office and one copy to be carried by the employee.

(3) The material shall be covered by a Classified Cover Sheet, DOT F 1600.7, or equivalent, placed in double, opaque sealed envelopes or wrappings, and fully addressed.

(4) The individual shall be briefed on his responsibilities to protect the material.

(5) The individual shall be given a letter prepared on official stationery and signed by the chief of the security staff or head of the activity, identifying the employee, authorizing

him to carry classified material, and briefly describing the physical characteristics of the envelope or wrappings, and the addressee and addressor. This authorization letter, together with official travel orders, should ordinarily permit the individual to travel without the need for subjecting the classified material to inspection. If difficulty is encountered outside the United States during Customs inspection, the individual should refuse to disclose the classified material and should insist on the assistance of the local U.S. diplomatic or military representative.

(6) Upon completion of the visit, the employee shall have the material forwarded to his office by approved means. All material taken for the purpose of the visit shall obtain a receipt.

c. Personnel may be authorized to remove classified material required in connection with local visits provided:

(1) The material is not available at the activity to be visited,

(2) the material is placed in double, opaque sealed, addressed envelopes (a brief case may suffice for the outer envelope),

(3) the employee is briefed on his responsibilities to protect the information, and

(4) the material is accounted for upon his return.

177. RESERVED.

SECTION 3. SPECIAL PROCEDURES FOR HAND-CARRYING CLASSIFIED INFORMATION ON COMMERCIAL PASSENGER AIRCRAFT

178. PROHIBITIONS. Hand-carrying of classified information on commercial passenger aircraft is discouraged. Classified information shall not be carried in checked luggage that will be transported in the aircraft, or which will be otherwise separated from the courier. If at all possible, classified information should be mailed in advance of the trip to a recipient having an authorized storage capability. Classified information **SHALL NOT** be hand-carried any place outside the United States or its possessions. Arrangements must be made by the servicing security element with Department of State and/or Armed Forces Courier Service for transport and secure storage of information at the desired destination.

179. BASIC REQUIREMENTS. If it is absolutely necessary that an FAA employee hand-carry classified information aboard commercial passengers aircraft and none of the prohibitions in paragraph 172 apply, then:

a. Advance and continued coordination shall be made with the air carrier(s) and terminal officials to develop mutually satisfactory arrangements. The servicing security element shall be contacted for assistance in making arrangements at the flight screening point.

b. The individual designated as courier shall be in possession of the appropriate DOT/FAA picture identification card or credential and a written authorization to hand-carry classified information.

c. The courier shall be briefed as to the provisions of this section.

180. PROCEDURES FOR CARRYING CLASSIFIED INFORMATION IN ENVELOPES. Persons carrying classified information should process through the airline ticketing and boarding procedure in the same manner as all other passengers.

a. The classified information shall contain no metal bindings and shall be in sealed envelopes, which shall be routinely offered for inspection for weapons. The screening official may check the envelope by X-raying machine, flurrying, feel, weight, etc., without opening the envelope itself.

b. Opening or reading of the classified document by the screening official is not authorized.

181. PROCEDURES FOR TRANSPORTING CLASSIFIED INFORMATION IN PACKAGES. Should it be necessary to transport large amounts or bulky items of classified information by commercial air carrier, the servicing security element shall provide procedural guidance.

182. DOCUMENTATION. When authorized to carry classified information aboard commercial air carriers, the courier shall have the original of a letter authorizing him/her to carry the information. The letter shall be prepared on FAA letterhead stationary, and shall;

a. Give the full name of the courier and his employing region/center.

b. Describe the type of identification the courier will present (including I.D card number, if any).

c. Describe the material being carried (e.g., three sealed packages, 9" X 8" X 24", addressee and addressor).

d. Identify the point of departure, destination and known transfer points.

e. Include a date of issue and an expiration date.

f. Include the name, title, and signature of the official issuing the letter. The letter should be signed by the servicing security element division chief; however, it may be signed by the courier's division or facility chief. Each envelope or package to be exempt shall be signed on its face by the official who signed the letter.

g. Include the name and telephone number of the office or facility designated to confirm the letter of authorization. The telephone number shall be an official U.S. Government number.

183. RESERVED.

SECTION 4. DISPOSAL AND DESTRUCTION OF CLASSIFIED MATERIAL

184. DISCUSSION. There are two basic concepts inherent in disposal. First, when the need for a specific item of classified material no longer exists, the item shall be disposed of. **THE LONGER AN INDIVIDUAL CLASSIFIED ITEM IS KEPT THE GREATER THE POTENTIAL FOR ITS COMPROMISE.** Second, **CLASSIFIED MATERIAL MUST BE DESTROYED BY SECURE MEANS TO PREVENT LOSS OR COMPROMISE.**

185. AUTHORIZED DISPOSAL.

a. Order 1350.14A, Records Organization, Transfer and Destruction Standards, together with supplementing and implementing directives and instructions, prescribed what record material shall be kept permanently, i.e., forwarded to the Federal record repositories, and what record material may be destroyed after required retention periods have been met, i.e., records disposal schedules. These directives apply to classified as well as unclassified documents. Accordingly, **OFFICES DESIRING TO DISPOSE OF CLASSIFIED MATERIAL SHALL REFER TO APPROPRIATE RECORDS MANAGEMENT INSTRUCTIONS.** Non-record copies of classified documents may be forwarded to the appropriate Security Control Point for destruction, at any time, at the discretion of the office holding the documents; however, care should be taken to assure that record material is not commingled with it prior to destruction.

b. Classified material to be disposed of by sending it to a records repository shall be reviewed for regrading, accounted for, packaged, and transmitted in accordance with appropriate provisions established in other chapters to this Order.

c. Provided the above requirements are met, classified material shall be destroyed when an office holding it no longer has an operational need for it and a future need is not foreseen. Such action will reduce the potential for compromise and costs attendant to protecting and storing it.

186. PROCEDURES LEADING TO DESTRUCTION.

a. Documents. All classified documents to be destroyed shall be forwarded to the Security Control Point for destruction. For TOP SECRET and SECRET documents, preparation of DOT Form 1600.4, which itemizes the documents, is required. The appropriate FAA Form 1600.35 shall be annotated to reflect the destruction of all classified material. The Security Control Point shall destroy or arrange for the destruction of the documents. The Security Control Point will assume that documents received for destruction are eligible for destruction from a records management standpoint. Except for classified waste (see sub-paragraph b below), the DOCUMENT SHALL NOT BE TORN OR MUTILATED BY THE OFFICE REFERRING THEM TO THE SECURITY CONTROL POINT.

b. Waste. All waste material containing classified information, such as carbon sheets, typewriter ribbons, plates, stencils, masters, stenographic and handwritten notes, and drafts which have not been entered into the accountability system shall be forwarded promptly to the Security Control Point for destruction. Waste material need not be itemized. The covering envelope shall be marked "CLASSIFIED WASTE". Until destroyed, classified waste is to be protected and stored in the same manner as accountable material of the same classification level.

c. Equipments. Offices having non-document type material to be destroyed shall consult with (1) the Security Control Point to assure that accountability and destruction records are executed and (2) the appropriate security element to assure that an adequate method for destruction is used. Offices are also responsible for assuring that the material is eligible for destruction from a property management standpoint.

d. Exception for Top Secret and COMSEC Material. TOP SECRET material, including waste, will be referred to the Top Secret Control Officer (TSCO) for destruction rather than the Security Control Point (in those activities where the TSCO and the Security Control Point Officer are not the same). COMSEC shall be returned to the COMSEC account custodian.

187. METHODS OF DESTRUCTION. THE BASIC CRITERION FOR DESTROYING CLASSIFIED MATERIAL IS THAT DESTRUCTION SHALL BE SO COMPLETE TO MAKE IMPOSSIBLE THE RECOVERY OF CLASSIFIED INFORMATION FROM THE RESIDUE. Destruction shall be accomplished by one of the following methods:

a. Burning. Documents shall be burned completely. Care shall be taken to assure that ashes are shifted and that no unburned pieces either remain or are allowed to escape by wind or draft.

b. Pulping, Pulverizing, Chopping or Shredding. Pulping must be complete. Documents destroyed by pulverizing or chopping must be reduced to bits no larger than 5 mm in any dimension. Only security approved shredders may be used. Servicing security elements shall be consulted prior to use and/or procurement of such equipment.

c. Melting, Chemical Decomposition, Mutilation. Non-documentary material may be destroyed by these means provided reconstruction is not possible. The appropriate headquarters security staff will provide guidance on the method and manner of destruction dependent upon the nature of the material to be destroyed. Destruction may be limited, where feasible, to those components of the material which actually contain the classified information.

d. Other. In certain instances, such as magnetic tapes, and microfiche classified information may be removed without destroying the medium on which it is recorded. Only those devices and methods which have been approved specifically from a security standpoint shall be used to erase or remove classified information. For specific guidance in this area, the servicing security element should be consulted.

188. DESTRUCTION OFFICIALS. The Security Control Point operator, or TSCO, as appropriate, shall destroy classified material. An additional person, cleared to the level of the material being destroyed, shall witness the destruction of material classified TOP SECRET and SECRET. A witness is not required for the destruction of material classified CONFIDENTIAL. The destruction officials shall be trained in the operations of the equipment being used for destruction and shall assure that destruction is accomplished to meet the standards prescribed in paragraph 181 above.

189. RECORDS.

a. Officials destroying TOP SECRET and SECRET material shall execute a destruction certificate reflecting:

- (1) date of destruction
- (2) identity of material, e.g., control number, description, etc., and
- (3) signatures of the destroying and witnessing officials.

b. Destruction certificates shall be filed at the control point for a period of no less than four years. Other accountability records maintained by the control point shall be annotated to reflect the destruction. A destruction certificate is not required for CONFIDENTIAL material, but accountability records (FAA Form 1600-35) shall be annotated.

190. RESERVED.

CHAPTER 2. FOREIGN GOVERNMENT AND INTERNATIONAL
ORGANIZATION INFORMATION

SECTION 1. CLASSIFICATION, DECLASSIFICATION AND MARKING
OF FOREIGN GOVERNMENT INFORMATION

191. DEFINITION. To be foreign government information within the meaning of Executive Order 12065, the information must be determined to be in one of two categories:

a. Information provided to the U.S. by a foreign government or international organization of governments, such as the North Atlantic Treaty Organization (NATO), where the U.S. has undertaken an obligation, expressed or implied, to keep the information in confidence. The information is considered to have been provided in confidence if it is marked in a manner indicating it is to be treated in confidence or if the circumstances of delivery indicate that the information is to be kept in confidence.

b. Information requiring confidentiality produced by the U.S. pursuant to a written joint agreement with a foreign government or international organization. A written joint agreement may be evidenced by an exchange of letters, a memorandum of understanding, or other informal written record of the joint agreement.

192. CLASSIFYING FOREIGN GOVERNMENT INFORMATION.

a. Foreign government information that is classified by a foreign entity shall either retain its original classification designation or be marked with a U.S. classification designation that will ensure a degree of protection equal to that required by the entity that provided the information.

b. Foreign government information that was not classified by a foreign entity but was provided to FAA with the expressed or implied obligation to hold it in confidence must be classified. The two-step procedure for classification prescribed in chapter 2 does not apply to the classification of such information. Careful consideration must be given to the sensitivity of the subject matter and the impact of its unauthorized disclosure upon both the U.S. and the originating foreign government or international organization to determine the most appropriate level of classification. E.O. 12065 states that a presumption of at least identifiable damage to the national security in the event of unauthorized disclosure of foreign government

information will be the guiding force in such matters. Therefore, such information shall be classified AT LEAST at the CONFIDENTIAL level. Original classification authority is not required for this purpose. However, if an FAA official determines that the information warrants a higher classification, he shall consult the servicing security element prior to assigning a higher classification to such information.

193. DURATION OF CLASSIFICATION. Foreign government information is exempt from the declassification requirements prescribed for U.S. classified information. Unless guidelines have been developed in consultation with the Archivist of the U.S., the Department of State, and the foreign government involved, foreign government information shall not be assigned a date or event for declassification but shall be assigned a date for review for declassification thirty years from the time the information was originated by the foreign government or acquired or classified by the FAA, whichever is earlier.

194. DECLASSIFICATION OF FOREIGN GOVERNMENT INFORMATION. In weighing the need to protect foreign government information and confidential foreign sources against the possible public interest in disclosure, the need to protect such information shall be presumed to predominate.

195. MARKING FOREIGN GOVERNMENT INFORMATION. Foreign security classifications generally parallel U.S. classifications (see Appendix 1). If the classification of foreign government documents is shown in English, no additional marking is required. If the foreign classification is not prescribed in English, the equivalent U.S. designation shall be entered on the material.

196. RESERVED.

SECTION 2. INTERNATIONAL ORGANIZATION INFORMATION

197. NATO AND CENTO CLASSIFIED INFORMATION.

a. The North Atlantic Treaty Organization (NATO) and the Central Treaty Organization (CENTO) each has issued a body of security regulations for the protection of classified material belonging to the respective organization. These regulations are applicable to every member state of the organization and require that each member designate a National Security Authority to assure the security of the information within that member nation. The Secretary of Defense has been appointed the Security Authority for the United States for these purposes.

b. The U.S. Security Authority for NATO Affairs has issued USSAN Instruction 1-69, Implementation of NATO Security Procedures. The U.S. Security Authority for CENTO Affairs has issued USSAC Instruction 1-68, Implementation of CENTO Security Procedures. These Instructions, or superseding editions, are effective within FAA and, together with the provisions of this order, shall be followed for the control and protection of classified material belonging to the respective treaty organization while in the custody of FAA.

198. CONTROL OF INTERNATIONAL ORGANIZATION INFORMATION. A Central U.S. Registry for each of the treaty organizations has been established under the Secretary of the Army and is the main receiving and dispatching authority for the U.S. for material belonging to the respective organization. A system of subregistries or control points has been established within each agency requiring material of this nature. In the FAA, a subregistry has been established within the office of Investigations and Security.

a All classified NATO or CENTO material shall flow through these subregistry or control points which, together with the appropriate security staff, shall assure that the information is controlled and protected in accordance with prescribed requirements.

b In this regard, no person shall be given access to NATO or CENTO classified information unless he has been specifically authorized for such access and briefed on his responsibilities to protect the information. This access authorization is in addition to any other clearance or authorization he may have. Order 1600.1B sets forth procedures for the issuance of these access authorizations.

199. RESERVED.

BLANK FRAME

FOR

PROPER PAGINATION

CHAPTER 9. VISIT CONTROL

SECTION 1. GENERAL PROVISIONS

200. DEFINITION OF VISITOR. The term visitor as used herein for security purposes applies as follows:

- a. A visitor to an FAA activity is any person who is not attached to or employed by the activity.
- b. The term visitor also includes personnel on temporary duty orders.

201. INCOMING VISITS.

a. The initial determination to be made on a proposed classified visit is whether the visit could be received without discussing or disclosing classified information. The activity receiving the visit must be provided with sufficient details as to the purpose of the visit in order for this determination to be made. If such data is not set forth in the visit request, the activity shall request it before the visit on a classified basis is approved. These details are required also for the activity receiving the visit to determine the extent of the classified information to be disclosed.

b. Normally, the responsibility for approving visit requests rests with the specific office to be visited. In the event the proposed visit is disapproved, or additional information is needed in order to assess more fully the visit request, the requestor should be promptly notified to that effect. Since approval of the proposed visit usually constitutes authority for the disclosure of classified information during the visit, sound judgment must be exercised when evaluating the proposed visitor's need for the information and for the visit itself.

c. A visit request should be in writing. In exceptional cases, however, the request may be accepted by phone or other rapid means of communication provided that it is confirmed later in writing. (Visit requests received by wire qualify as written communication and do not require confirmation.)

202. VISITOR CATEGORIES. For security control purposes visitors are placed into the following categories, each of which has slightly different procedural requirements:

a. Personnel of the Executive Branch of the Government Involved in Day-to-Day Relations with Members of the FAA Activity to be Visited and Personally Known to Them. No formal visit

notifications are needed but each person receiving such a visit is responsible for assuring that the visitor has a requirement for the classified information involved and that he is cleared to the appropriate level.

b. Personnel of the Executive Branch Other than the Above.

(1) The visit request should contain the following information:

- (a) Name in full, military rank where appropriate, title or position.
- (b) Citizenship, date and place of birth.
- (c) Employer or sponsor if other than the originator of the visit request.
- (d) Name and address of the activity to be visited if other than the address on the visit application.
- (e) Date, time and duration of proposed visit.
- (f) Purpose of visit in detail, including estimated degrees of access required.
- (g) Security clearance status of the visitor and the clearing agency.
- (h) Names of persons to be visited if known.

(2) Visits of this category may be approved by the head of the activity or office being visited or his designee. The certificate of clearance contained in an official visit request from another agency of the government should be accepted.

c. Contractor Employees Who are Currently Cleared Under the Industrial Security Program Administered by the Department of Defense.

(1) Contractors have been instructed to submit visit requests to the heads of government activities or specific offices to be visited. Visit requests are to contain the following information:

- (a) Name and address of activity to be visited.
- (b) Name and title of person(s) to be visited, if known.

(c) Name of the proposed visitor, his date and place of birth and citizenship.

(d) Job title or position of the proposed visitor.

(e) Requesting contractor's certification of the clearance status of the proposed visitor to include degree, date and issuing authority.

(f) Purpose of and justification for the visit in detail including contract or program on which visitor is engaged and under which the visit is necessary and the identification of classified information to which access is required, if known.

(g) Date of proposed visit or period during which the request is to be valid.

(h) Name and address of the requesting contractor or User Agency activity.

(i) Level of requesting contractor's facility clearance and date granted.

(j) Name and address of requesting contractor's cognizant security office, including telephone number if known.

(2) Additionally, a contractor is directed to furnish a statement from his Government contracting officer attesting that the visit and release of classified information in connection therewith is essential to the performance of the contract or program.

(3) Visits in this category may be approved by the head of the activity or office being visited or his designee. A cleared contractor's certification of the clearance of his employee may be accepted without further confirmation. In this regard, cleared contractors have been authorized to grant their employees CONFIDENTIAL clearances. Accordingly, the contractor's cognizant security office would have no record of this type of clearance.

d. U.S. Citizens on Unofficial Business and non-Communist Bloc or Aligned Foreign Nationals and Foreign Representatives. Visits in this category may be approved by the head of the activity or office being visited or his designee. Visitors in this category shall not have access to classified information, oral or visual, without the written approval of ASE-1.

e. Visitors from Communist Bloc or Aligned Countries. Visits in this category shall be coordinated through the International Liaison Officer, AIA-30 and ASE-200 and approved by these offices

before access may be granted to any FAA facility, equipment or information. These visitors shall not be given access to any classified information.

203. IDENTIFICATION. Approved visitors shall present adequate identification at the time of the visit. The office being visited shall not permit the visitor to have access to classified information until satisfied as to his identity. If there is any questions, the government agency, contractor, or sponsor whom he represents should be contacted for confirmation.

204. VISITOR LOGS. A visitor log or register (FAA Form 1600-8) shall be maintained as determined by the individual activity.

205. RESTRICTIONS OF MOVEMENT. Offices or activities receiving visitors shall assure that the visitors are given access only to that classified information for which they have been authorized to receive during the visit. Visitors shall be escorted in those areas wherever, if not escorted, they could possibly gain unauthorized access to classified information. The designated escort should be a responsible, appropriately cleared employee who has been informed regarding the visitor's access limitations and restrictions placed on the visitor's movement. As a general rule, visits of tour groups and guests to FAA activities will be guided by an appropriate escort.

206. RECORDINGS AND PHOTOGRAPHS. Visitors shall not be permitted to make recordings of classified discussions or take photographs in areas where classified information might be recorded on the film, except with the approval of and in accordance with specific guidance from the security element serving the activity.

207. REPORT OF UNUSUAL VISITOR INTEREST. If a visitor expresses an unusual interest in information that he is not authorized to receive, or expresses feelings inimical to the best interests of the U.S., the head of the activity concerned shall transmit immediately a complete report of the circumstances to the servicing security element for subsequent referral through ASE-200 to M-50. These reports shall include the following:

- a. Full name and title or position of visitor.
- b. Nationality.
- c. Sponsor.
- d. Authority for visit.
- e. Items of particular interest to the visitor.

- f. General type of questions asked.
- g. Expressed object of the visit.
- h. Estimate of the real object of the visit.
- i. General estimate of ability, intelligence and technical knowledge of the visitor.
- j. Exactly what was shown, explained, and refused.

208. OUTGOING VISITS. Arrangements for visits by FAA personnel to other government agencies and contractors should be made sufficiently in advance of the proposed visit to permit processing of the visit request.

a. DOT Form 1600-15, Visit Clearance, shall be prepared in triplicate by the operating element initiating the visit and provided to the servicing security element for review, certification, and transmittal.

b. Visits to DOT Activities and Other Government Agencies. A visit request containing the information prescribed in paragraph 198 will be forwarded to the activity or office to be visited.

c. Visits to Contractor Facilities. If the proposed visit involves an FAA classified contract, the visit request containing the information required by paragraph 198 will be sent directly to the contractor. If an FAA contract is not involved, the request will be directed to the contractor through the government contracting officer when known.

209. RESERVED.

SECTION 2. INTRA-FAA VISITS

210. DISCUSSION. The use of DOT Form 1600-15 is specifically intended for notification of a visit that requires access to classified information and/or material. In the past this form has been utilized for intra-FAA visits and visits to other governmental organizations or firms of the private sector. With the full implementation of the security data in the PHIS, the need to use the DOT Form 1600-15 for intra-FAA visits of employees normally no longer exists. Region/center security elements have access to Personnel Management Information System terminals and can verify security clearance data on employees in a time sensitive manner. The use of DOT Form 1600-15 will be continued for security clearance certifications to non-FAA entities.

211. INTRA-FAA VISITS. The office or facility being visited shall notify the servicing security element as soon as they become aware of an employee visit that involves a requirement for access to classified information or material in order that the security clearance data in the PMIS can be verified and provided. The name, social security number, facility to be visited, level of access required, and the inclusive dates of visit must be provided to the servicing security element. The PMIS shall provide hardcopy verification of security clearance data which shall then be certified by the region/center of headquarters security official and transmitted to the activity or facility to be visited.

212. RESERVED.

CHAPTER 10. COMPROMISES AND SECURITY VIOLATIONS

213. SUMMARY OF CONTROLS.

- a. Loss or compromise of classified information shall be reported immediately.
- b. Attempts shall be made to regain custody of the material.
- c. Determinations shall be made as to the significance of the incident.
- d. Action shall be taken, when possible, to counter the effects of the loss.
- e. Action shall be taken to correct the situation which gave rise to the loss.

214. VIOLATIONS OF SECURITY DIRECTIVES. The policies and procedures in this and related security directives are intended to prevent the compromise of classified information. The handling or dissemination of classified information contrary to the provisions of these directives could result in a compromise or possible compromise of the information. WHEREAS AN INFRACTION OF A SPECIFIC REQUIREMENT MAY NOT SUBJECT INFORMATION TO COMPROMISE IN ONE INSTANCE, AN INFRACTION OF THE SAME RULE UNDER DIFFERENT CIRCUMSTANCES COULD RESULT IN A COMPROMISE. For this reason, all violations of the directives shall be reported and corrective action taken.

215. INITIAL REPORTING AND RESPONSIBILITIES.

- a. Any employee, military personnel, or other person associated with FAA, such as detailees, consultants, etc., having knowledge of the loss, unauthorized disclosure, or possible compromise of classified information; or of an infraction of security regulations shall immediately advise his supervisor, higher authority, or the servicing security element. Supervisors or other officials who have been advised of the incident shall report or assure that the matter is reported immediately to the servicing security element.
- b. Depending upon the circumstances, personnel shall take action to recover the material and provide custody.
- c. Material which is pertinent to inquiries into the occurrence, evidence of tampering, etc. shall be kept intact and preserved.

216. ADMINISTRATIVE INQUIRIES. Administrative inquiries of minor infractions shall be conducted by the cognizant activity or office or by the servicing security element. If the inquiries establish that a loss of classified material did not occur or that the possibility of compromise was remote, the results of the inquiries together with a statement of corrective and/or disciplinary action taken shall be made a matter of record with the servicing security element.

217. ADDITIONAL NOTIFICATION AND INVESTIGATION.

a. If it appears that an actual compromise occurred or that the possibility of compromise cannot be discounted, the servicing security element shall immediately advise ASE-200 which, depending upon the circumstances and sensitivity of the affected information, shall notify the originating agency. A copy of this notification shall be forwarded by ASE-200 to M-50.

b. Unless directed to the contrary by the ASE-200, the reporting security element shall initiate a comprehensive investigation into the incident to determine, in essence, what happened; where, when, and how it happened; who was responsible; what was the identify and classification of all affected information; and what measures were taken to recover lost or misplaced material. The report of investigation shall also set forth an evaluation of the probability of compromise and of the significance of the incident from the standpoint of who had, or may have had, access to the information while it was unprotected.

c. The report of investigation shall be submitted to the head of the activity in which the incident occurred and to ASE-200 which shall forward a copy to the activity or agency which originated the affected material and to M-50.

218. ACTIONS SUBSEQUENT TO INVESTIGATION.

a. A FAA activity which is advised that information or material which it originated has been subjected to compromise shall take action as warranted by the circumstances, and as may be appropriate and feasible, to change portions of plans, programs, operations, etc., which may be affected in order to minimize the adverse consequences of compromise. Additionally, a classification review of the information shall be made to determine whether it should be regraded or declassified. Notification of changes in plans or classification shall be provided to holders of the material.

b. Corrective action to prevent the occurrence of similar violations shall be taken immediately. Corrective action would include, but is not limited to:

(1) changes in local practices relating to controlling classified information or more stringent enforcement of local practices;

(2) intensification of security orientation; and

(3) disciplinary action.

c. In determining the specific disciplinary action to be taken, officials shall be guided by an overall assessment of the occurrence, including such factors as the seriousness of the violation, the sensitivity of the information subjected to compromise, disregard and previous disregard of security or other administrative regulations, etc. Administrative actions are separate and apart from actions which may be taken against an individual if he violates applicable statutes dealing with unauthorized releases of classified information. When individual responsibility for the violation cannot be determined, but the facts indicate that a supervisor or other official allowed conditions to exist which led to the violation, responsibility shall be placed on that supervisor or official.

d. Corrective actions are subject to review by, and such additional actions it deems necessary, the Departmental Security Review Committee.

219. CLASSIFICATION OF REPORTS. Reports of violations and investigative reports will not normally be classified provided the report itself does not contain classified information. (For example, information that SECRET document XYZ has been subjected to compromise and the circumstance of the incident is not classified. If the report contains classified information taken from XYZ document, the report would be classified.)

a As an exception to this criterion, when classified information appears in the public news media or in other means of public dissemination, reports identifying such instances shall be classified, commensurate to the degree of the classified information involved in the apparent compromise, until an evaluation is made by cognizant authority whether to declassify the compromised information.

b If the determination is made in such an instance to retain the classification despite the compromise, reports of the incident similarly will remain classified. Likewise, reports which could help an unauthorized person to find lost or missing classified material normally shall be classified.

220. CRYPTOGRAPHIC INFORMATION. Possible compromises of cryptographic information or violations of crypto-operating or maintenance instructions will be handled also in accordance with requirements specified by the National Security Agency directive, KAG-1D.

Belgian, French and International Post Organization Security Classification

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	
Argentina	EXCLUSIVAMENTE SECRETO	SECRETO	CONFIDENTIAL	
Australia	TOP SECRET 3	SECRET	CONFIDENTIAL	
Austria	STRENG GEHEIM	GEHEIM	VERSCHEIDEN	MUN FÜR DEN DIENSTGEBRAUCH
Belgium (French)	TRÈS SECRET	SECRET	CONFIDENTIAL	DIFFUSION RESTREINTS
(Dutch)	ZIN GEHEIM	GEHEIM	VERTROUWELIJK	BEPERKT VERSPREIDING
Bolivia	SUPERSECRETO or NOT SECRETO	SECRETO	CONFIDENTIAL	
Brazil	ULTRA SECRETO	SECRETO	CONFIDENTIAL	RESERVADO
Cameroon	TRÈS SECRET	SECRET	SECRET/CONFIDENTIAL	
Canada	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Chile	SECRETO	SECRETO	RESERVADO	RESERVADO
Colombia (two systems)	NOT SECRETO EXCLUSIVAMENTE RESERVADO	SECRETO SECRETO	CONFIDENTIAL RESERVADO	CONFIDENTIAL RESERVADO
Costa Rica	ALTO SECRETO	SECRETO	CONFIDENTIAL	
Denmark	TRØST HØJEST	HØJEST	FORTROLIG	TIL FJERNSTE BRUG
Ecuador	SECRETISSIMO	SECRETO	CONFIDENTIAL	RESERVADO

2/5/80

2/5/80

Country	TOP SECRET	SECRET	CONFIDENTIAL	
Ireland	TOP SECRET AS-CONFIDENTIAL	SECRET CONFIDENTIAL	CONFIDENTIAL TERRA	RESTRICTED SQUADRA
Israel	TOP SECRET TM 72 7118	SECRET 7118	SECRET 7118	SECRET 72118
Italy	CONFIDENTIAL	SECRET	CONFIDENTIAL	CONFIDENTIAL
Japan	TOP SECRET 機密	SECRET 秘密	SECRET 秘密	RESTRICTED 取扱注意 RUOMR 部外秘
Jordan	TOP SECRET 1 & 7118 TOP SECRET	SECRET 1 & 7118 TOP SECRET	SECRET 1 & 7118 TOP SECRET	SECRET
Lebanon	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Luxembourg	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Netherlands	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
New Zealand	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Norway	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Poland	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Portugal	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED

[illegible]

[illegible]

NOTE: In all instances foreign security classification systems are not exactly parallel to the United States system and exact equivalent classifications cannot be stated. The classifications given above represent the nearest comparable designations which are used to signify degrees of protection and control similar to those prescribed for the equivalent United States classifications.

"ACROSS" information is an evaluative designation used by NATO to identify "Restricted Data" or "Formerly Restricted Data" information released by the Government of the United States to NATO.

2/5/80

1600.2B
Appendix 2

APPENDIX 2. FORMS LIST FOR ORDER 1600.2B

FORM NUMBER	TITLE
DOT Form 1600.4 Source of supply is FAA Depot Stock Number FSN 0052-684-20000(PD)	Classified Material Record
DOT Form 1600.6 Source of supply is FAA Depot Stock Number FSN 0052-409-2001(SE)	Lock Combination Record
DOT Form 1600.7 Source of supply is FAA Depot Stock Number FSN 0052-404-7000(SH)	Cover Sheet
DOT Form 1600-15 Source of supply is FAA Depot and GSA Supply Service Stock Number FSN 0052-687-5001	Visit Clearance
FAA Form 1600-8 Source of supply is FAA Depot Stock Number FSN 0052-672-4000(SH)	Visitor Register
FAA Form 2831 Source of supply is FAA Depot Stock Number FSN 0052-408-9000(SH)	Top Secret Information Disclosure Record
FAA Form 2833 Source of supply is FAA Depot Stock Number FSN 0052-409-1000(SE)	Report of Security Violation
DOT Form 1600.33 Source of supply is FAA Depot Stock Number FSN 0052-627-7001	Safe Check Record
DD Form 254 Source of supply is ASE-200	Contract Security Classification Specification
DOT Form 1600-35 Source of Supply is FAA Depot Stock Number FSN 0052-835-7000	Classified Document Register